Compact IBBE and Fuzzy IBE from Simple Assumptions

Junqing Gong, Benoît Libert, Somindu C Ramanna

Compact IBBE and Fuzzy IBE from Simple Assumptions

Junqing Gong[1], Benoît Libert[1,2], and Somindu C. Ramanna[3]

[1] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France
[2] CNRS, Laboratoire LIP, France
[3] Indian Institute of Technology, Kharagpur, India

Abstract. We propose new constructions for identity-based broadcast encryption (IBBE) and fuzzy identity-based encryption (FIBE) in bilinear groups of composite order. Our starting point is the IBBE scheme of Delerablée (Asiacrypt 2007) and the FIBE scheme of Herranz *et al.* (PKC 2010) proven secure under parameterised assumptions called generalised decisional bilinear Diffie-Hellman (GDDHE) and augmented multi-sequence of exponents Diffie-Hellman (aMSE-DDH) respectively. The two schemes are described in the prime-order pairing group. We transform the schemes into the setting of (symmetric) composite-order groups and prove security from two static assumptions (subgroup decision).

The Déjà Q framework of Chase *et al.* (Asiacrypt 2016) is known to cover a large class of parameterised assumptions (dubbed über assumption), that is, these assumptions, when defined in asymmetric composite-order groups, are implied by subgroup decision assumptions in the underlying composite-order groups. We argue that the GDDHE and aMSE-DDH assumptions are not covered by the Déjà Q über assumption framework. We therefore work out direct security reductions for the two schemes based on subgroup decision assumptions. Furthermore, our proofs involve novel extensions of Déjà Q techniques of Wee (TCC 2016-A) and Chase *et al.*

Our constructions have constant-size ciphertexts. The IBBE has constant-size keys as well and guarantees stronger security as compared to Delerablée's IBBE, thus making it the first compact IBBE known to be selectively secure without random oracles under simple assumptions. The fuzzy IBE scheme is the first to simultaneously feature constant-size ciphertexts and security under standard assumptions.

Keywords. Identity-based broadcast encryption, fuzzy IBE, space efficiency, simple assumptions.

1 Introduction

Identity-based encryption (IBE) [56] is a public-key paradigm where users' private keys are generated by trusted authorities and derived from some easy-to-remember string (like an email address) that serves as a public key so as to simplify key management. Attribute-based encryption (ABE) [55, 36] is a powerful extension of IBE where ciphertexts are labeled with a set of descriptive attributes (e.g., "hiring committee", "admin", ...) in such a way that decryption works whenever these attributes satisfy an access policy which is hard-coded in the decryption key.

Functional encryption (FE) [55, 16] is an extreme generalization of IBE, where a master private key SK allows deriving sub-keys SK_F associated with functions F. Given an encryption C of a message X, a sub-key SK_F allows computing $F(X)$ while revealing nothing else about X. The message $X = (\mathsf{ind}, M)$ usually consists of an index ind, which is essentially a set of attributes, and a message M, which is sometimes called "payload". While the latter is always computationally hidden, the index ind of a ciphertext may be public or private. Not surprisingly, schemes in the public index setting tend to be significantly more efficient in terms of ciphertext and key sizes.

In the private-index setting, anonymous IBE [11, 18] is an example of functional encryption for the equality testing functionality. In the public [55, 36] and private-index [40] cases, ABE can be cast as another particular flavour of FE, where private keys are associated with expressive access policies. These primitives provide fine-grained access control [55] or privacy-preserving searches over encrypted data [11, 1]. In its key-policy (KP-ABE) flavour, ABE involves private keys associated with a possibly complex Boolean expression F and, if the ciphertext encrypts the message $X = (\mathsf{ind}, M)$, the private key SK_F reveals M if and only if $F(\mathsf{ind}) = 1$. Ciphertext-policy ABE (CP-ABE) schemes proceed the other way around: ciphertexts are labeled with a policy F; private keys are associated with an attribute set ind and decryption succeeds whenever $F(\mathsf{ind}) = 1$.

The usual "collusion-resistance" requirement captures the intuition that no collection of private keys should make it possible to decrypt a ciphertext that none of these keys can individually decrypt. While properly defining the security of FE turns out to be non-trivial [16], the literature usually distinguishes selective adversaries [19] – that have to declare the index of the challenge ciphertext $\mathsf{ind}^\star$ upfront (even before seeing the master public key) – from adaptive adversaries, which can choose $\mathsf{ind}^\star$ after having made a number of private key queries for functions of their choice.

In terms of expressiveness, a major challenge is certainly to efficiently evaluate any polynomial-time-computable function F over encrypted data. While theoretical solutions achieve this goal using the obfuscation machinery [33], practical instantiations of functional encryption are only known for very restricted classes of functions (such as IBE [12, 59] or ABE [40]) for the time being.

Even for particular functionalities and selective adversaries, proving security is challenging when we seek to optimise the size of ciphertexts and keys. For example, squeezing many attributes in the same ciphertext component often comes at the price of larger private keys [6, 4] or security proofs under fancy q-type assumptions [10, 14] (or both). Likewise, short private keys and public parameters [41, 52] often entail strong, variable-size assumptions. Eventualy, constant-size ciphertexts or keys ("constant" meaning that it only depends on the security parameter and not on the number of adversarial queries or features of the system) often translate into non-constant-size assumptions. In some situations, information theoretic arguments [32] even rule out the possibility of simultaneously achieving constant-size ciphertexts and keys, no matter which assumption is considered.

Here, we restrict ourselves to specific functionalities for which we are interested in proving the security of *compact* schemes under well-studied, constant-size assumptions. By "compact", we mean that ciphertexts can be comprised of a *constant* number of group elements – no matter how many

attributes or users are associated with them – without inflating the private key size. In particular, private keys should be no longer than in realisations of the same functionality without short ciphertexts. Finally, we aim at avoiding the caveat of relying on variable-size, q-type assumptions, which should notoriously be used with caution [25].

We achieve this goal for two natural extensions of IBE, which are known as *identity-based broadcast encryption* (IBBE) [2, 53] and *fuzzy identity-based encryption* (FIBE) [55]. In the former, ciphertexts are encrypted for a list of identities. The latter is an ABE for policies consisting of a single threshold gate: i.e., ciphertexts and private keys both correspond to a set of attributes and decryption succeeds whenever the two sets have a sufficiently large intersection. In fact, IBBE and FIBE can both be seen as special cases of CP-ABE for policies consisting of a single gate: an IBBE is nothing but a CP-ABE for one OR gate, which is implied by FIBE for 1-out-of-n gates. However, considering the two primitives separately allows obtaining shorter private keys in the IBBE case.

1.1 Our Contribution

We describe the first IBBE system with a security proof under constant-size assumptions and that simultaneously features constant-size ciphertexts and private keys. In our scheme, only the size of public parameters depends on the maximal number n of receivers per ciphertext. Users' private keys only consist of a single(!) group element while ciphertexts are only longer than plaintexts by 2 elements of a composite-order group. We prove selective security in the standard model under subgroup assumptions [43] in bilinear groups of order $N = p_1p_2p_3$. In comparison, all earlier IBBE realisations with short ciphertexts either incur $O(n)$-size private keys [2, 15, 5, 48] or combine the random oracle model [8] with very *ad hoc* assumptions [53, 27] tailored to the result to be proved.

As a second contribution, we extend our IBBE scheme into a fuzzy IBE system with $O(1)$-size ciphertexts and private keys made of $O(\ell)$ group elements, where ℓ is the maximal number of attributes per identity. Our FIBE scheme thus asymptotically achieves the same private key size as [55] with the benefit of constant-size ciphertexts, regardless of the number of ciphertext attributes. In contrast, except [37], previously known KP-ABE systems with short ciphertexts either inflate private keys by a factor $O(\ell)$ [6, 48, 7, 50] or are restricted to small attribute universes [38].

While our constructions rely on composite order groups where pairings are rather expensive to compute [31], they only require two pairing evaluations on behalf of the receiver (and no pairing on the sender's side). Our schemes are proved selectively secure using the Déjà Q technique of Chase and Meiklejohn [23], which was re-used by Wee [63] and refined by Chase *et al.* [24]. In Appendix A, we provide detailed comparisons of our schemes with previously known realizations.

1.2 Overview of our Techniques

Our identity-based broadcast encryption scheme is obtained by instantiating (a variant of) Delerablée's IBBE [27] in composite order groups and providing a direct security proof, analogously to Wee's IBE [63]. In prime order groups, Delerablée's construction [27] is proved selectively secure in the random oracle model under a highly non-standard q-type assumption, where q simultaneously depends on the number of private key queries and the maximal number of receivers per ciphertext. While this assumption is a special case of the Uber assumption of Boneh, Boyen and Goh [10], it seems to escape the family of assumptions that reduce the constant-size subgroup assumptions via the framework of Chase, Maller and Meiklejohn [24]: in Section 3.1, we indeed explain why the results of [24] alone do not immediately guarantee the security of Delerablée's IBBE in composite

order groups.[4] Moreover, even if they did, a direct instantiation of [27] in composite order groups would only be guaranteed to be secure in the random oracle model.[5] In contrast, we give a direct proof of selective security in the standard model.

Just like [27, 63], our scheme uses the private key generation technique of the Sakai-Kasahara IBE [54], which computes inversions in the exponent. Letting $\mathbb{G}$ be a group of order $N = p_1p_2p_3$ with subgroups of order p_i for each $i \in \{1, 2, 3\}$, if $g^\gamma \in \mathbb{G}_{p_1}$ and $G_i = g^{(\alpha^i)} \in \mathbb{G}_{p_1}$ are part of the public parameters, a private key for the identity id consists of $\mathsf{SK}_{\mathsf{id}} = u^{\gamma/(\alpha+\mathsf{id})} \cdot X_{p_3}$, where $u \in \mathbb{G}_{p_1}$ belongs to the master secret key and $X_{p_3} \in_R \mathbb{G}_{p_3}$. If $S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$ denotes the set of authorised receivers, one of the ciphertext components packs their identities into one group element $g^{s \cdot \prod_{i \in S}(\alpha+\mathsf{id})}$, which can be seen as a randomised version of Nguyen's accumulator [46]. As shown in [27], by introducing $g^{\gamma \cdot s}$ in the ciphertext and blinding the message as $M \oplus \mathsf{H}(e(g,u)^{\gamma \cdot s})$, we can enable decryption by exploiting the divisibility properties of the polynomial $p_S(\alpha) = \prod_{i \in S}(\alpha + \mathsf{id})$, analogously to [46]. Like the security proof of Wee's IBE [63], our proof proceeds by first introducing $\mathbb{G}_{p_2}$ components in ciphertexts. Then, following the technique of [23], it uses the entropy of $\alpha, \gamma \bmod p_2$ – which are information theoretically hidden by g^γ and $G_i = g^{(\alpha^i)}$ – to gradually introduce $\mathbb{G}_{p_2}$ components of the form $g_2^{\sum_{j=1}^k \tilde{\gamma} \cdot r_j \cdot p_S(\alpha_j)/(\alpha_j+\mathsf{id})}$, where $\{r_j\}_{j=1}^k$ are shared by all private keys. At each step, we can increase the number of terms in the exponent so that, when k is sufficiently large, all keys $\mathsf{SK}_{\mathsf{id}}$ have independent random components of order p_2. At this point, an information theoretic argument shows that the ciphertext statistically hides the plaintext.

The crucial step of the proof consists of arguing that the newly introduced term in the sum $\sum_{j=1}^k r_j \cdot p_S(\alpha_j)/(\alpha_j + \mathsf{id})$ is statistically independent of the public parameters. At this step, our information theoretic argument differs from Wee's [63] because, in our IBBE system, public parameters contain additional group elements of the form $U_i = u^{\alpha^i} \cdot R_{3,i}$, which inherit $\mathbb{G}_{p_2}$ components that depend on $\sum_{j=1}^k r_j \cdot \alpha_j^i \bmod p_2$, for the same coefficients $r_j \in \mathbb{Z}_{p_2}$ as those showing up in private keys. Since private keys and public key components $\{U_i\}_{i=1}^n$ have correlated semi-functional components[6] that share the same $\{r_j \bmod p_2\}_{j=1}^k$, we have to consistently maintain this correlation at all steps of the sequence of game and argue that, when we reach the final game, the $\mathbb{G}_{p_2}$ components of $\mathsf{SK}_{\mathsf{id}_1}, \ldots, \mathsf{SK}_{\mathsf{id}_q}$ and $\{U_i\}_{i=1}^n$ are uncorrelated in the adversary's view. In Wee's constructions [63], this is done by arguing that matrices of the form $(\alpha_j^i)_{i,j \in [q]}$ or $\big(1/(\alpha_j + \mathsf{id}_i)\big)_{i,j}$ are invertible. Here, we are presented with more complex square matrices that involve the two kinds of entries and also depend on the polynomial $p_{S^\star}(\alpha) = \prod_{\mathsf{id} \in S^\star}(\alpha + \mathsf{id})$, where $S^\star$ is the set of the target identities. More precisely, these matrices contain sub-matrices of the form $\big(p_{S^\star}(\alpha_i)/(\alpha_i + \mathsf{id}_j)\big)_{i,j}$, where id_j denotes the j-th private key query. We use the property that the overall square matrices are invertible over $\mathbb{Z}_{p_2}$ as long as none of the first-degree $(\alpha + \mathsf{id}_j)$ divides $p_{S^\star}(\alpha)$ (i.e., $\mathsf{id}_j \notin S^\star$ for all private key queries id_j). When this is the case, we are guaranteed that the $\mathbb{G}_{p_2}$ components of ciphertexts, private keys and public parameters are i.i.d. in the adversary's view.

Our fuzzy IBE construction is an adaptation of the system described by Herranz, Laguillaumie and Ràfols [37, 4] in prime order groups, which is itself inspired by the dynamic threshold encryption

[4] We believe our arguments showing that the assumptions under question are not covered by the Déjà Q framework are sufficient. Also, we do not know if there exist other parameterised assumptions in this class that could possibly be used to prove security of the IBBE and FIBE schemes.

[5] Alternatively, the scheme of [27] can be proved secure in the standard model if the adversary also announces all its private keys queries (in addition to the target set of identities) before seeing the public parameters.

[6] The proof of Wee's broadcast encryption [63, Section 4] has a similar correlation between the $\mathbb{G}_{p_2}$ components of private keys and public parameters but, in the final step, the statistical argument involved simpler-to-analyse Vandermonde matrices.

primitive of Delerablée and Pointcheval [28] and relies on a similarly strong assumption. The FIBE system of [37] modifies [27, 28] by randomizing the generation of private keys. In our construction, private keys for an attribute set $\{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$ similarly consist of

$$\left(K_i = u^{\frac{\gamma}{\alpha+\mathsf{id}_i}} \cdot X_{3,i}\right)_{i=1}^{\ell}, \qquad \left(K'_i = u^{\alpha^i} \cdot X'_{3,i}\right)_{i=1}^{n-1}, \qquad K_0 = u \cdot u_0 \cdot X_{3,0},$$

where $u \in_R \mathbb{G}_{p_1}$ and $X_{3,i} \in_R \mathbb{G}_{p_3}$ are freshly chosen for each key and $u_0 \in \mathbb{G}_{p_1}$ is a master secret key component which is committed via $e(g, u_0)^\gamma$ in the master public key. Intuitively, the public parameters $u_0^{\alpha^i} \cdot R_{3,i}$ of Delerablée's IBBE are now replaced by similar-looking private key components $K'_i = u^{\alpha^i} \cdot X'_{3,i}$ for random $u \in_R \mathbb{G}_1$ that are used in K_0 to blind the master secret key u_0 (collusion-resistance is ensured by the fact that distinct keys involve fresh randomizers u).

Due to the strong structural similarity, the proof for the selective security of our fuzzy IBE can be viewed as an extension of that for our IBBE system. From the viewpoint of reduction, the fresh $u \in \mathbb{G}_{p_1}$ in each secret key allows us to correspond each secret key to a fresh IBBE instance and analyse them in an independent fashion. In particular, by considering K_i as $\mathsf{SK}_{\mathsf{id}_i}$ and K'_i as U_i, we can apply the proof method of our IBBE to introduce independent random $\mathbb{G}_{p_2}$ component in all these components and K_0 (with $u_0 \cdot X_{3,0}$). As discussed earlier, the core step is again to argue the invertibility of a matrix of some special form for each secret key. Although the matrices we are considering now look like those for the IBBE system, the situation is actually more complex. More specifically, the matrices contain sub-matrices of the form $(p_{S^\star,\tau^\star}(\alpha_i)/(\alpha_i + \mathsf{id}_j))_{i,j}$ where $p_{S^\star,\tau^\star}(\alpha) = \prod_{\mathsf{id} \in S^\star}(\alpha + \mathsf{id}) \cdot \prod_{i \in [\delta]}(\alpha + d_i)$ where $S^\star$ is the set for the target fuzzy identity, $(d_i)_i$ is a set of dummy identities and δ depends on the target threshold τ^*. Unlike the IBBE case, there can be an $\mathsf{id}_j \in \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$ such that $\mathsf{id}_j \in S^\star$ so that $(\alpha + \mathsf{id}_j)$ divides $p_{S^\star,\tau^\star}(\alpha)$ in the FIBE case. This prevents us from directly applying our previous result on the matrices. Instead, we will prove the property that these matrices are still invertible as long as the number of such id_j do not exceed the target threshold τ^*. Inspired by the recent proof for IBE in the multi-instance setting [20], we can in fact change the distributions of all secret keys *independently* but *simultaneously* using the random self-reducibility of decisional subgroup assumptions. Once we have independent random $\mathbb{G}_{p_2}$ component in K_0 in each secret key, we then introduce semi-functional component (in $\mathbb{G}_{p_2}$) for the master secret key component u_0 and show that it will be hidden by the random $\mathbb{G}_{p_2}$ component in K_0. This means the semi-functional component of u_0 will only appear in the challenge ciphertext which is adequate for proving the selective security of our fuzzy IBE system.

1.3 Related Work

Broadcast encryption was introduced by Fiat and Naor [30] and comes either in combinatorial [44] or algebraic flavors [45, 14, 34, 60, 41]. One of the most appealing tradeoffs was given in the scheme of Boneh, Gentry and Waters [14], which features short ciphertexts and private keys but linear-size private keys in the total number of users. While its security was initially proved under a parameterised assumption, recent extensions [63, 24] of the Déjà Q framework [23] showed how to prove the security (against static adversaries) of its composite-order-group instantiations under constant-size subgroup assumptions. Boneh *et al.* suggested a variant [17] of the BGW scheme [14] with polylogarithmic complexity in all metrics using multi-linear maps. Unfortunately, the current status of multi-linear maps does not enable secure instantiations of [17] for now (see, e.g., [26]).

Identity-based broadcast encryption was formally defined by Abdalla, Kiltz and Neven [2] and independently considered by Sakai and Furukawa [53]. One of the salient advantages of IBBE over

traditional public-key broadcast encryption is the possibility of accommodating an exponential number of users with polynomial-size public parameters. IBBE was recently used [29] in the design of efficient 0-RTT key exchange protocols with forward secrecy. Abdalla *et al.* [2] gave a generic construction with short ciphertexts and private keys of size $O(n^2)$, where n is the maximal number of receivers. Sakai and Furukawa [53] suggested a similar construction to [27] with security proofs in the generic group and random oracle model. Boneh and Hamburg [15] obtained a system with $O(1)$-size ciphertexts and $O(n)$-size keys. Using the Déja Q technique, Chen *et al.* [21] described an identity-based revocation mechanism [41] with short ciphertexts and private keys under constant-size assumptions. The aforementioned constructions were all only proven secure against selective adversaries. Gentry and Waters [34] put forth an adaptively secure construction based on q-type assumptions while Attrapadung and Libert [5] showed a fully secure variant of [15] under simple assumptions. To our knowledge, the only IBBE realisations that simultaneously feature constant-size ciphertexts and private keys are those of [27, 53], which require highly non-standard assumptions and the random oracle model. As mentioned by Derler *et al.* [29], the short ciphertexts and private keys of Delerablée's scheme [27] make it interesting to instantiate their generic construction of Bloom Filter Encryption, which in turn implies efficient 0-RTT key exchange protocols. Until this work, even for selective adversaries, it has been an open problem to simultaneously achieve short ciphertext and private keys without resorting to variable-size assumptions.

Attribute-based encryption was first considered in the seminal paper by Sahai and Waters [55]. Their fuzzy IBE primitive was later extended by Goyal *et al.* [36] into more expressive forms of ABE, where decryption is possible when the attribute set of the ciphertext satisfies a more complex Boolean formula encoded in the private key. After 2006, a large body of work was devoted to the design of adaptively secure [42, 47–49, 7, 50, 58] and more expressive ABE systems [51, 41, 61, 62, 35, 13]. In contrast, little progress has been made in the design of ABE schemes with short ciphertexts. The first reasonably expressive ABE systems with constant-size ciphertexts were given in [37, 6, 4] under q-type assumptions. The solution of Herranz *et al.* [37] is a fuzzy IBE (i.e., a CP-ABE system for one threshold gate) with private keys of size $O(n)$ where n is the maximal number of attributes per ciphertext. The more expressive KP-ABE systems of [6, 4] support arbitrary Boolean formulas, but enlarge the private keys of [36] by a factor n. The construction of [38, Section 3.4] eliminates the upper bound on the number of ciphertext attributes, but lengthens private keys by a factor $|U|$, where U is the universe of attributes. Several follow-up works improved upon [6] by proving security under simple assumptions [22, 57] or achieving full security [7]. However, all known KP-ABE schemes with short ciphertexts under simple assumptions suffer from similarly large private keys. While our scheme only supports one threshold gate, it turns out to be the first solution with short ciphertexts under simple assumptions that avoids blowing up private keys by a factor $O(n)$.

2 Preliminaries

NOTATION. We write $x_1, \ldots, x_k \xleftarrow{R} \mathcal{X}$ to indicate that $x_1, \ldots, x_k$ are sampled independently and uniformly from the set $\mathcal{X}$. For a PPT algorithm $\mathcal{A}$, $y \xleftarrow{R} \mathcal{A}(x)$ means that y is chosen according to the output distribution of $\mathcal{A}$ on input x. For integers $a < b$, $[a, b]$ denotes the set $\{x \in \mathbb{Z} : a \leq x \leq b\}$ and we let $[b] = [1, b]$. If $\mathbb{G}$ is a cyclic group, $\mathbb{G}^\times$ denotes the set of generators of $\mathbb{G}$.

2.1 Composite-Order Pairings and Hardness Assumptions

A (symmetric) composite-order pairing ensemble generator $\mathsf{GroupGen}()$ is an algorithm that inputs a security parameter η and an integer m and returns an $(m+3)$-tuple $\mathcal{G} = (p_1, \ldots, p_m, \mathbb{G}, \mathbb{G}_T, e)$

where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = p_1 \cdots p_m$ (a square-free, hard-to-factor integer) and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate and efficiently computable bilinear map. The primes are chosen so that $p_i > 2^\eta$ for $i \in \{1, 2, 3\}$. We will use hardness assumptions which require the factorisation of N to remain hidden. Given $\mathcal{G} = (p_1, \ldots, p_m, \mathbb{G}, \mathbb{G}_T, e)$, let $\mathcal{G}_{\text{pub}} = (N, \mathbb{G}, \mathbb{G}_T, e)$ denote the public description of $\mathcal{G}$ where $N = p_1 \cdots p_m$ and we assume that $\mathbb{G}, \mathbb{G}_T$ contain respective generators (of the full groups). Letting $\mathbb{G}_{p_i}$ be the subgroup of order p_i of $\mathbb{G}$, we denote elements of $\mathbb{G}_{p_i}$ with subscript i for $i \in [m]$. We now describe decisional subgroup (DS) assumptions w.r.t. $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\eta, 3)$, which is stated in terms of two distributions: $\mathcal{D}, T_1$ and $\mathcal{D}, T_2$. We define $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\text{DS}}(\eta) = |\Pr[\mathscr{B}(\mathcal{D}, T_1) = 1] - \Pr[\mathscr{B}(\mathcal{D}, T_2) = 1]|$ to be the advantage of a distinguisher $\mathscr{B}$ against DS. We now describe $\mathcal{D}, T_1, T_2$ for the assumptions we use.

Assumption DS1. Pick generators $g_1 \xleftarrow{\text{R}} \mathbb{G}_{p_1}^\times$ and $g_3 \xleftarrow{\text{R}} \mathbb{G}_{p_3}^\times$. Define $\mathcal{D} = (\mathcal{G}_{\text{pub}}, g_1, g_3)$, $T_1 \xleftarrow{\text{R}} \mathbb{G}_{p_1}$ and $T_2 \xleftarrow{\text{R}} \mathbb{G}_{p_1 p_2}$. DS1 holds if for all PPT $\mathscr{B}$, $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\text{DS1}}(\eta)$ is negligible in η.

Assumption DS2. Pick $g_1 \xleftarrow{\text{R}} \mathbb{G}_{p_1}^\times$, $g_3 \xleftarrow{\text{R}} \mathbb{G}_{p_3}^\times$, $h_{12} \xleftarrow{\text{R}} \mathbb{G}_{p_1 p_2}$ and $h_{23} \xleftarrow{\text{R}} \mathbb{G}_{p_2 p_3}$. Define $\mathcal{D} = (\mathcal{G}_{\text{pub}}, g_1, g_3, h_{12}, h_{23})$, $T_1 \xleftarrow{\text{R}} \mathbb{G}_{p_1 p_3}$ and $T_2 \xleftarrow{\text{R}} \mathbb{G}_{p_1 p_2 p_3}$. The DS2 assumption holds if for all PPT $\mathscr{B}$, $\mathsf{Adv}^{\mathscr{B}}_{\mathcal{G},\text{DS2}}(\eta)$ is negligible in η.

2.2 Identity-Based Broadcast Encryption (IBBE)

Definition 1 (IBBE). *An IBBE scheme is defined by probabilistic algorithms* Setup, KeyGen, $\mathsf{Encrypt}$ *and* $\mathsf{Decrypt}$. *The identity space is denoted by* $\mathcal{I}$ *and the message space is denoted by* $\mathcal{M}$.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** *Takes as input a security parameter* λ, *the maximum number* n $(= \mathsf{poly}(\lambda))$ *of recipient identities in a broadcast and generates the public parameters* PP *and the master secret* MSK. *The algorithm also defines the identity space* $\mathcal{I}$ *and message space* $\mathcal{M}$.

$\mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id})$**:** *Inputs an identity* id *and* MSK*; outputs a key* $\mathsf{SK}_{\mathsf{id}}$ *for* id.

$\mathsf{Encrypt}(\mathsf{PP}, S \subseteq \mathcal{I}, m \in \mathcal{M})$**:** *Takes as input the public parameters and a set of identities* S *intended to receive the message* m. *If* $|S| \leq n$, *the algorithm outputs the ciphertext* CT.

$\mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}, \mathsf{SK}_{\mathsf{id}})$**:** *Inputs* PP, *a set* $S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$, *an identity* id, *a secret key* $\mathsf{SK}_{\mathsf{id}}$ *for* id, *a ciphertext* CT *and outputs a message* $m' \in \mathcal{M}$ *if* $\mathsf{id} \in S$ *and otherwise outputs* $\perp$.

Correctness. The IBBE scheme satisfies correctness if, for all sets $S \subseteq \mathcal{I}$ with $|S| \leq n$, for all identities $\mathsf{id}_i \in S$, for all messages $m \in \mathcal{M}$, if $(\mathsf{PP}, \mathsf{MSK}) \xleftarrow{\text{R}} \mathsf{Setup}(1^\lambda, 1^n)$, $\mathsf{SK}_{\mathsf{id}_i} \xleftarrow{\text{R}} \mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id}_i)$ and $\mathsf{CT} \xleftarrow{\text{R}} \mathsf{Encrypt}(\mathsf{PP}, S, m)$, then we have $\Pr[m = \mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}_i, \mathsf{SK}_{\mathsf{id}_i})] = 1$.

Definition 2 (IBBE Security). *An IBBE system* $\mathcal{IBBE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *provides selective security if no PPT adversary* $\mathscr{A}$ *has non-negligible advantage in the following game.*
Initialise: $\mathscr{A}$ *commits to a target set of identities* $S^* = \{\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*\}$.
Setup: *The challenger runs the* Setup *algorithm of* $\mathcal{IBBE}$ *and gives* PP *to* $\mathscr{A}$.
Key Extraction Phase 1: $\mathscr{A}$ *makes key extraction queries. For a query on an identity vector* id *such that* $\mathsf{id} \notin S^*$, *the challenger runs* $\mathcal{IBBE}.\mathsf{KeyGen}$ *algorithm and responds with a key* $\mathsf{SK}_{\mathsf{id}}$.
Challenge: $\mathscr{A}$ *provides two messages* m_0, m_1. *The challenger chooses a bit* β *uniformly at random from* $\{0, 1\}$, *computes* $\mathsf{CT}^* \xleftarrow{\text{R}} \mathcal{IBBE}.\mathsf{Encrypt}(\mathsf{PP}, S^*, m_\beta)$ *and returns* CT^* *to* $\mathscr{A}$.
Key Extraction Phase 2: $\mathscr{A}$ *makes more key extraction queries with the restriction that it cannot query a key for any identity in* S^*.
Guess: $\mathscr{A}$ *outputs a bit* β'. *If* $\beta = \beta'$, *then* $\mathscr{A}$ *wins the game. The adversary* $\mathscr{A}$*'s advantage is given by the distance* $\mathsf{Adv}^{\mathscr{A}}_{\mathcal{IBBE},\mathsf{sid\text{-}cpa}}(\lambda) = |\Pr[\beta = \beta'] - 1/2|$.

2.3 Fuzzy Identity-Based Encryption (FIBE)

Definition 3 (FIBE). *A fuzzy IBE scheme is defined by probabilistic algorithms –* Setup, KeyGen, Encrypt *and* Decrypt. *The identity space is denoted by* $\mathcal{I}$ *and the message space is denoted by* $\mathcal{M}$.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** *Takes as input a security parameter* λ*, the maximum size* n $(= \mathsf{poly}(\lambda))$ *of sets associated with ciphertexts and generates the public parameters* PP *and the master secret* MSK. *The algorithm also defines the identity space* $\mathcal{I}$ *and message space* $\mathcal{M}$.

$\mathsf{KeyGen}(\mathsf{MSK}, S \subseteq \mathcal{I})$**:** *Inputs a set* S *and* MSK*; outputs a secret key* SK_S *for* S.

$\mathsf{Encrypt}(\mathsf{PP}, S \subseteq \mathcal{I}, \tau, m \in \mathcal{M})$**:** *Takes as input the public parameters* PP*, a set of identities* S *along with a threshold* τ *and a message* m. *If* $\tau \leq |S| \leq n$*, the algorithm outputs the ciphertext* $\mathsf{CT}_{S,\tau}$.

$\mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}_{S,\tau}, S', \mathsf{SK}_{S'})$**:** *This algorithm inputs the public parameters* PP*, a set* $S \subseteq \mathcal{I}$ *with a threshold* τ *and a ciphertext* $\mathsf{CT}_{S,\tau}$ *associated with them, another set* $S' \subseteq \mathcal{I}$ *and its corresponding secret key* $\mathsf{SK}_{S'}$*, outputs a message* $m' \in \mathcal{M}$ *if* $|S \cap S'| \geq \tau$ *and* $\perp$ *otherwise.*

Correctness. The FIBE scheme is correct if, for all sets $S \subseteq \mathcal{I}$, all thresholds $\tau \leq |S| \leq n$, all $S' \in \mathcal{I}$ satisfying $|S \cap S'| \geq \tau$, all $m \in \mathcal{M}$, when $(\mathsf{PP}, \mathsf{MSK}) \xleftarrow{\mathrm{R}} \mathsf{Setup}(1^\lambda, 1^n)$, $\mathsf{SK}_{S'} \xleftarrow{\mathrm{R}} \mathsf{KeyGen}(\mathsf{MSK}, S')$ and $\mathsf{CT}_{S,\tau} \xleftarrow{\mathrm{R}} \mathsf{Encrypt}(\mathsf{PP}, S, \tau, m)$, then $\Pr[m = \mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}_{S,\tau}, S', \mathsf{SK}_{S'})] = 1$.

Definition 4 (FIBE Security). *A FIBE system* $\mathcal{FIBE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *provides selective security if no PPT adversary* $\mathscr{A}$ *has non-negligible advantage in the following game.*
Initialise: $\mathscr{A}$ *commits to a target set* $S^* \subseteq \mathcal{I}$ *and threshold* τ^* *satisfying* $\tau^* \leq |S^*| \leq n$.
Setup: *The challenger runs the* Setup *algorithm of* $\mathcal{FIBE}$ *and gives* PP *to* $\mathscr{A}$.
Key Extraction Phase 1: $\mathscr{A}$ *makes a number of key extraction queries. For a query on* $S \subseteq \mathcal{I}$ *such that* $|S^* \cap S| < \tau^*$*, the challenger runs* $\mathsf{SK}_S \leftarrow \mathcal{FIBE}.\mathsf{KeyGen}$ *and otuputs* SK_S.
Challenge: $\mathscr{A}$ *provides two messages* m_0, m_1*. The challenger chooses* $\beta \xleftarrow{\mathrm{R}} \{0,1\}$*, computes* $\mathsf{CT}^* \xleftarrow{\mathrm{R}} \mathcal{FIBE}.\mathsf{Encrypt}(\mathsf{PP}, S^*, \tau^*, m_\beta)$ *and returns* CT^* *to* $\mathscr{A}$.
Key Extraction Phase 2: $\mathscr{A}$ *makes more key extraction queries with the restriction that it cannot query a key for any set* S *such that* $|S^* \cap S| \geq \tau^*$.
Guess: $\mathscr{A}$ *outputs a bit* β'*. We say* $\mathscr{A}$ *wins the game if* $\beta = \beta'$*. The advantage of* $\mathscr{A}$ *in winning the* sid-cpa *game is defined to be* $\mathsf{Adv}^{\mathscr{A}}_{\mathcal{FIBE},\mathsf{sid\text{-}cpa}}(\lambda) = |\Pr[\beta = \beta'] - 1/2|$.

3 Compact IBBE from Subgroup Decision Assumptions

This section describes our IBBE scheme with short ciphertexts and keys. The structure is similar to Delerablée's IBBE [27] in asymmetric prime-order groups.

3.1 Déjà Q Framework and its implications on Delerablée's IBBE

The scheme proposed by Delerablée in [27] is based on prime-order asymmetric pairings and offers constant-size ciphertexts and keys. However, its proof of security relies on random oracles and a parameterised assumption called generalised decisional Diffie-Hellman exponent (GDDHE) with instances containing $O(q+n)$ group elements. A scheme/proof without random oracles is also suggested but at the cost of an interactive GDDHE-like assumption and a more restrictive security definition (called IND-na-sID-CPA) in which the adversary has to commit to the identities for key extract queries during the initialisation phase (in addition to the challenge identity set).

It is natural to ask whether the scheme can be lifted to the composite-order setting and proved secure based on subgroup decision assumptions via the Déjà Q framework [23, 24]. That is, we ask whether the Uber assumption in asymmetric composite-order bilinear groups defined in [24] covers the GDDHE assumption or not? The answer is negative. To see why, let us take a closer look at the Uber assumption of [24] and the (asymmetric) GDDHE-assumption. For clarity, we avoid formal descriptions of assumptions and other details.

Uber assumption [24]. Assume $\mathcal{G} = (N, p_1, p_2, p_3, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ be an asymmetric composite-order pairing group. Let $R(\boldsymbol{x}), S(\boldsymbol{x}), V(\boldsymbol{x})$ denote sets of polynomials in n variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ and let $z(\boldsymbol{x})$ be a polynomial in $\boldsymbol{x}$. Let g be a generator of $\mathbb{G}_1$ and $h, \hat{h}$ be two independent generators of $\mathbb{G}_2$. The uber assumption states that given

$$g, \hat{h}, g^{R(\boldsymbol{x})}, h^{S(\boldsymbol{x})}, e(g,h)^{V(\boldsymbol{x})}, T$$

it is hard to decide if $T = e(g,\hat{h})^{z(\boldsymbol{x})}$ or $T \in_R \mathbb{G}_T$. It known [24] that the uber assumption is implied by constant-size subgroup decision assumptions in $\mathbb{G}_1$ and $\mathbb{G}_2$ if $R(\boldsymbol{x}), z(\boldsymbol{x})$ are linearly independent along other requirements (see [24, Proposition 3.9] for formal statement).

In order to simplify our analysis, we may let $\hat{h}^\delta = h$ for an independent exponent $\delta \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and re-state the uber assumption as: given

$$g, \hat{h}, g^{R(\boldsymbol{x})}, \hat{h}^{\delta \cdot S(\boldsymbol{x})}, e(g,\hat{h})^{\delta \cdot V(\boldsymbol{x})}, T$$

it is hard to decide if $T = e(g,\hat{h})^{z(\boldsymbol{x})}$ or $T \in_R \mathbb{G}_T$. Here, $\delta \cdot S(\boldsymbol{x}) = \{\delta \cdot s(\boldsymbol{x}) : s \in S(\boldsymbol{x})\}$ and $\delta \cdot V(\boldsymbol{x}) = \{\delta \cdot v(\boldsymbol{x}) : v \in V(\boldsymbol{x})\}$. We highlight that the Déjà Q framework in [24] requires the polynomials in the exponents of $\hat{h}$ to be in the form of $\delta \cdot \mathsf{poly}(\boldsymbol{x})$ with an independent δ.

Déjà Q framework does not cover GDDHE assumption [27]. Let an asymmetric prime-order pairing configuration $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Let g_0, h_0 be the respective generators of $\mathbb{G}_1, \mathbb{G}_2$. Pick $k, \gamma \xleftarrow{\mathrm{R}} \mathbb{Z}_p$ and let f, g be two co-prime polynomials with pairwise distinct roots of respective orders q, n. The GDDHE assumption states that given

$$g_0, g_0^{\gamma}, g_0^{\gamma^2}, \ldots, g_0^{\gamma^{q-1}}, g_0^{\gamma f(\gamma)}, g_0^{k\gamma f(\gamma)}, \qquad h_0, h_0^{\gamma}, h_0^{\gamma^2}, \ldots, h_0^{\gamma^{2n}}, h_0^{kg(\gamma)},$$

along with $T \in \mathbb{G}_T$, it is hard to determine whether $T = e(g_0, h_0)^{kf(\gamma)}$ or $T \in_R \mathbb{G}_T$.

As a direct attempt to put GDDHE into the Déjà Q framework, we can let $g = g_0$ and $\hat{h} = h_0$. This means we are considering $\boldsymbol{x} = (\gamma, k)$ and

$$z(\gamma, k) = kf(\gamma),\ V = \emptyset,\ R(\gamma, k) = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-1}, \gamma f(\gamma), k\gamma f(\gamma)\}.$$

In this case, polynomials in the exponents of $\hat{h}$ include $\{1, \gamma, \gamma^2, \ldots, \gamma^{2n}, kg(\gamma).\}$ Since both γ and k has appeared in $z(\boldsymbol{x})$ and $R(\boldsymbol{x})$, there's no means to write these polynomials in the form of $\delta \cdot \mathsf{poly}(\boldsymbol{x})$ with an independent variable δ.

With our current choice of g, all polynomials in the exponents of g fit the Déjà Q framework quite well. To get around this problem, we try another definition of $\hat{h}$. The best choice can be setting $\hat{h} = h_0^k$, $\boldsymbol{x} = \gamma$ and $z(\gamma) = f(\gamma)$. The basic idea is to set $\delta = k^{-1}$. However, the polynomials in the exponents of $\hat{h}$ become

$$k^{-1}, k^{-1} \cdot \gamma, k^{-1} \cdot \gamma^2, \ldots, k^{-1} \cdot \gamma^{2n}, g(\gamma)$$

where the last polynomial is still in the wrong form and we can not publish $\hat{h}$ itself this time. Even worse, δ will also appear in the exponent of $g = g_0$ since the input to the adversary contains $g^{k\gamma f(\gamma)}$ (in the original assumption) which will become $g^{\delta^{-1}\gamma f(\gamma)}$ in the current setting. We can make this argument more general. If we want to borrow δ from $kf(\gamma)$, which seems to be the

unique random source we can use in the challenge, it will finally appear (in some form) in the term $g^{k\gamma f(\gamma)}$. Therefore, the Déjà Q transform fails.

In this forthcoming sections, instead of trying to reduce subgroup decision to the GDDHE, we give direct security reductions (via Déjà Q techniques) for constructions in composite-order groups (similar to [27]) from subgroup decision assumptions. Our construction has constant-size ciphertexts and keys and is selectively secure under the static subgroup decision assumptions, thus achieving a stronger security guarantee as compared to [27].

3.2 Construction

We now describe the construction $\mathit{IBBE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** Let $\mathcal{M} = \{0,1\}^\rho$ where $\rho \in \mathsf{poly}(\lambda)$. Generate a composite-order pairing ensemble $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\rho + 2\lambda, 3)$. Set $N = p_1p_2p_3$ and $\mathcal{I} = \mathbb{Z}_N$. Pick generators $g, u \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ and $g_3 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. Sample $R_{3,i} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ for $i = [n]$. Also, choose $\alpha, \gamma \xleftarrow{\mathrm{R}} \mathbb{Z}_N$. Let $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$ be a universal hash function with output length ρ. Define the master secret as $\mathsf{MSK} = (u, \alpha, \gamma, g_3)$ while the public parameters consist of

$$\mathsf{PP} = \big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^\gamma,\ (G_i = g^{\alpha^i},\ U_i = u^{\alpha^i} \cdot R_{3,i})_{i=1}^n,\ e(g,u)^\gamma,\ \mathsf{H}\big).$$

$\mathsf{KeyGen}(\mathsf{MSK}, \mathsf{id})$**:** Pick $X_3 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ and generate the key for identity id as $\mathsf{SK}_{\mathsf{id}} = u^{\frac{\gamma}{\alpha+\mathsf{id}}} \cdot X_3$.

$\mathsf{Encrypt}(\mathsf{PP}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}, M)$**:** To encrypt $M \in \{0,1\}^\rho$ for the set S, expand the polynomial $p_S(x) = \prod_{i=1}^{\ell}(x + \mathsf{id}_i) = \sum_{j=0}^{\ell} c_j x^j \in \mathbb{Z}_N[x]$. Choose $s \xleftarrow{R} \mathbb{Z}_N$ and output

$$\mathsf{CT} = \big(\, C_0 = M \oplus \mathsf{H}(e(g,u)^{s\gamma}), \quad C_1 = g^{s\gamma}, \quad C_2 = \Big(g^{c_0} \cdot \textstyle\prod_{j=1}^{\ell} G_j^{c_j}\Big)^s = g^{s \cdot p_S(\alpha)}\,\big).$$

$\mathsf{Decrypt}(\mathsf{PP}, S, \mathsf{CT}, \mathsf{id}, \mathsf{SK}_{\mathsf{id}})$**:** If $\mathsf{id} \notin S$, return $\perp$. Otherwise, $p_S(x)/(x+\mathsf{id}) = p_{S\setminus\{\mathsf{id}\}}(x) = \sum_{i=0}^{\ell-1} z_i x^i$ is a polynomial, where $z_0 = \prod_{\mathsf{id}_i \in S\setminus\{\mathsf{id}\}} \mathsf{id}_i$. Output $M = C_0 \oplus \mathsf{H}\big((A_2/A_1)^{1/z_0}\big)$, where

$$A_1 = e(C_1, \prod_{j=1}^{\ell-1} U_j^{z_j}) = e(g^{s\gamma}, u^{p_{S\setminus\{\mathsf{id}\}}(\alpha) - z_0}) = e(g,u)^{s\gamma(p_{S\setminus\{\mathsf{id}\}}(\alpha) - z_0)},$$

$$A_2 = e(C_2, \mathsf{SK}_{\mathsf{id}}) = e(g^{sp_S(\alpha)}, u^{\frac{\gamma}{\alpha+\mathsf{id}}} \cdot X_3) = e(g,u)^{s\gamma p_{S\setminus\{\mathsf{id}\}}(\alpha)}.$$

The correctness of the scheme follows from the divisibility properties of $p_S(x)$ and is easy to verify.

3.3 Proof of Security

In the security reduction, we use an additional parameter $U_0 = u \cdot R_{3,0}$ where $R_{3,0} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ that is not part of either PP or MSK.

Theorem 1. *For any adversary $\mathscr{A}$ attacking IBBE in the* sid-cpa *model making at most q key extraction queries, there exist algorithms $\mathscr{B}_1, \mathscr{B}_2$ such that*

$$\mathsf{Adv}^{\mathscr{A}}_{\mathit{IBBE},\mathsf{sid\text{-}cpa}}(\lambda) \le 2 \cdot \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda) + (q+n+2) \cdot \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda) + \tfrac{(q+n+1)^2}{p_2} + \tfrac{1}{p_2} + \tfrac{1}{2^\lambda}.$$

Proof. We organise the proof as a sequence of $2(q+n)+8$ hybrid games. Let $E_\square$ denote the event that $\mathscr{A}$ wins in $\mathsf{G}_\square$. Let $\mathsf{id}_1, \ldots, \mathsf{id}_q$ denote the identities provided in extract queries.

G_r: This is the real security game.

G_0: This game is like G_r with the following modifications regarding private key queries.
- No two distinct identities $\mathsf{id} \neq \mathsf{id}'$ mod N satisfy $\mathsf{id} \equiv \mathsf{id}'$ mod p_2.
- $\mathscr{A}$ does not provide any id such that $\alpha + \mathsf{id} \equiv 0 \bmod p_1$.

These events can be detected without knowing the factorization of N, by a simple gcd calculation (indeed, since PP only reveal α mod p_1 we can only have $\alpha+\mathsf{id} \equiv 0$ mod N with negligible probability). If either of these rules is broken, the challenger aborts the game. Assuming that N is hard to factor, these modifications do not affect $\mathscr{A}$'s view. Since Assumptions DS1 and DS2 imply the hardness of factoring N, we have $|\Pr[E_r]-\Pr[E_0]| \leq \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda)+\mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda)$.

G_1: This is similar to G_0 with the following changes. Let $S^* = \{\mathsf{id}^*_1, \ldots, \mathsf{id}^*_{\ell^*}\}$ be the set of challenge identities chosen by $\mathscr{A}$. In the setup phase, we pick $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and set $\gamma = \tilde{\gamma} \cdot p_{S^*}(\alpha) \bmod N$. The public parameters and challenge ciphertext are generated as in G_0 (as the challenger knows γ). Upon a query on id_y ($y \in [q]$), the secret key is computed as

$$\mathsf{SK}_{\mathsf{id}_y} = u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot X_{3,y},$$

where $X_{3,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. Since this is only a conceptual change, we have $\Pr[E_0] = \Pr[E_1]$.

G_2: In this game, the session key is generated using the parameter U_0 and the component C^*_1 of the challenge ciphertext is sampled at random from $\mathbb{G}_{p_1}$.

$$C^*_1 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}, \qquad C^*_2 = {C^*_1}^{1/\tilde{\gamma}}, \qquad C^*_0 = M_\beta \oplus \mathsf{H}(e(C^*_1, U_0)),$$

where $\beta \xleftarrow{\mathrm{R}} \{0,1\}$ and $U_0 = u \cdot R_{3.0}$ with $R_{3,0} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. If we write $C^*_1 = g^{s\gamma}$ for some uniformly random $s \in_R \mathbb{Z}_{p_1}$, then C^*_2 is given by $(C^*_1)^{1/\tilde{\gamma}} = g^{s\gamma/(\gamma/p_{S^*}(\alpha))} = g^{s p_{S^*}(\alpha)}$ and is thus well-formed. Also, C^*_0 has the correct distribution since

$$C^*_0 = M_\beta \oplus \mathsf{H}(e(C^*_1, U_0)) = M_\beta \oplus \mathsf{H}(e(g^{s\gamma}, u \cdot R_{3,0})) = M_\beta \oplus \mathsf{H}(e(g,u)^{s\gamma}).$$

The modifications G_1 are thus conceptual and hence $\Pr[E_1] = \Pr[E_2]$.

G_3: This game is identical to G_2 except that C^*_1 is sampled uniformly in $\mathbb{G}_{p_1 p_2}$. Other components of the challenge ciphertext and the secret keys are generated as in G_2.

Lemma 1. *There is a PPT algorithm $\mathscr{B}_1$ such that $|\Pr[E_2] - \Pr[E_3]| \leq \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda)$.*

G_4: We change the distribution of parameters $\{U_i\}_{i=0}^n$ and secret keys $\mathsf{SK}_{\mathsf{id}_1}, \ldots, \mathsf{SK}_{\mathsf{id}_q}$ by gradually introducing $\mathbb{G}_{p_2}$ components. This is done via sub-games $\mathsf{G}_{4.k.0}$, $\mathsf{G}_{4.k.1}$ for $k \in [q+n+1]$ defined as follows. For convenience, we define $\mathsf{G}_{4.0.1} = \mathsf{G}_3$ and $\mathsf{G}_{4.(q+n+2).1} = \mathsf{G}_4$.

- In $\mathsf{G}_{4.k.0}$, change the distribution of U_i for $i \in [0,n]$ as follows.

$$u^{\alpha^i} \cdot g_2^{\sum_{j=1}^{k-1} r_j \alpha_j^i} \cdot R_{3,i} \quad \longrightarrow \quad u^{\alpha^i} \cdot \boxed{g_2^{r\alpha^i}} \cdot g_2^{\sum_{j=1}^{k-1} r_j \alpha_j^i} \cdot R_{3,i}$$

  Also, change the distribution of the secret key $\mathsf{SK}_{\mathsf{id}_y}$ for a query on id_y for $y \in [q]$:

$$u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot g_2^{\sum_{j=1}^{k-1} \frac{r_j \cdot \tilde{\gamma} \cdot p_{S^*}(\alpha_j)}{\alpha_j + \mathsf{id}_y}} \cdot X_{3,y} \longrightarrow u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot \boxed{g_2^{\frac{r \cdot \tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}}} g_2^{\sum_{j=1}^{k-1} \frac{r_j \cdot \tilde{\gamma} \cdot p_{S^*}(\alpha_j)}{\alpha_j + \mathsf{id}_y}} \cdot X_{3,y}$$

- In $\mathsf{G}_{4.k.1}$ ($k \in [0, q+n+1]$), the distribution of $\{U_i\}_{i \in [0,n]}$ and keys $\{\mathsf{SK}_{\mathsf{id}_y}\}_{y \in [q]}$ is now

$$U_i = u^{\alpha^i} \cdot g_2^{\sum_{j=1}^{k} r_j \cdot \alpha_j^i} \cdot R_{3,i}, \qquad \mathsf{SK}_{\mathsf{id}_y} = u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot g_2^{\sum_{j=1}^{k} \frac{r_j \cdot \tilde{\gamma} \cdot p_{S^*}(\alpha_j)}{\alpha_j + \mathsf{id}_y}} \cdot X_{3,y}.$$

The following lemma shows that $\mathsf{G}_{4.(k-1).1}$ and $\mathsf{G}_{4.k.0}$ are computationally indistinguishable.

Lemma 2. *There is a PPT algorithm $\mathscr{B}_2$ such that $|\Pr[E_{4.(k-1).1}]-\Pr[E_{4.k.0}]| \leq \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda)$.*

In the transition from $\mathsf{G}_{4.k.0}$ to $\mathsf{G}_{4.k.1}$, α and r in the exponent of g_2 are replaced by random $\alpha_k, r_k \in_R \mathbb{Z}_{p_2}$. This change does not affect $\mathscr{A}$'s view since none of the other public parameters or the challenge ciphertext reveal $\alpha \bmod p_2$. In particular, due to the change introduced in G_2, C_2^* is computed using $\tilde{\gamma}$, which is independent of $p_{S^*}(\alpha) \bmod p_2$ since PP only reveals $\tilde{\gamma} \cdot p_{S^*}(\alpha) \bmod p_1$ via g^γ and $e(g,u)^\gamma$. Hence, by the CRT, we can replace $\alpha \bmod p_2$ by $\alpha_k \bmod p_2$ without $\mathscr{A}$ noticing. As a result, we have $\Pr[E_{4.k.0}] = \Pr[E_{4.k.1}]$ for each $k \in [0, n+q+2]$.

G_5: We replace the exponents in the $\mathbb{G}_{p_2}$-components of $\mathsf{SK}_{\mathsf{id}_1}, \ldots, \mathsf{SK}_{\mathsf{id}_q}$ and $\{U_i\}_{i=0}^n$ by independent random elements $t_0, t_1, \ldots, t_{q+n} \in \mathbb{Z}_{p_2}$. Namely, $(U_i)_{i=0}^n$ and keys are computed as

$$U_i = u^{\alpha^i} \cdot \boxed{g_2^{t_i}} \cdot R_{3,i} \quad \forall i \in [0,n], \qquad \mathsf{SK}_{\mathsf{id}_y} = u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot \boxed{g_2^{t_{n+y}}} \cdot X_{3,y}.$$

We argue that G_5 is statistically close to G_4. We consider the $\mathbb{G}_{p_2}$ components of $U_0, U_1, \ldots, U_n, \mathsf{SK}_{\mathsf{id}_1}, \ldots, \mathsf{SK}_{\mathsf{id}_q}$. In G_4, their logarithms $t'_0, \ldots, t'_{n+q} \in \mathbb{Z}_{p_2}$ w.r.t. g_2 are

$$\begin{pmatrix} t'_0 \\ t'_1 \\ \vdots \\ t'_n \\ t'_{n+1} \\ \vdots \\ t'_{n+q} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q+n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_{q+n+1}^n \\ \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_1)}{\alpha_1 + \mathsf{id}_1} & \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_2)}{\alpha_2 + \mathsf{id}_1} & \cdots & \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_{q+n+1})}{\alpha_{q+n+1} + \mathsf{id}_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_1)}{\alpha_1 + \mathsf{id}_q} & \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_2)}{\alpha_2 + \mathsf{id}_q} & \cdots & \frac{\tilde{\gamma} \cdot p_{S^*}(\alpha_{q+n+1})}{\alpha_{q+n+1} + \mathsf{id}_q} \end{pmatrix}}_{\mathbf{A}} \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{q+n+1} \end{pmatrix}. \tag{1}$$

Since $\mathsf{id}_y \notin S^*$ for all $y \in [q]$, the modifications introduced in G_0 ensure that none of the first-degree polynomials $(x + \mathsf{id}_y) \bmod p_2$ divides $p_{S^*}(x) \in \mathbb{Z}_{p_2}[x]$. In addition, remainders f_y obtained upon division of $p_{S^*}(x)$ by $x + \mathsf{id}_y$ are constant-degree non-zero polynomials (i.e., non-zero constants in $\mathbb{Z}_{p_2}$). Using elementary row and column operations on $\mathbf{A}$, we obtain that $\det \mathbf{A} = c \cdot \det \mathbf{B} \bmod p_2$, where $c = \tilde{\gamma}^q \cdot f_1 f_2 \cdots f_q$ and

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q+n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_{q+n+1}^n \\ \frac{1}{\alpha_1 + \mathsf{id}_1} & \frac{1}{\alpha_2 + \mathsf{id}_1} & \cdots & \frac{1}{\alpha_{q+n+1} + \mathsf{id}_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_1 + \mathsf{id}_q} & \frac{1}{\alpha_2 + \mathsf{id}_q} & \cdots & \frac{1}{\alpha_{q+n+1} + \mathsf{id}_q} \end{pmatrix}.$$

Lemma 3 provides an explicit computation of the determinant of $\mathbf{B}$.

Lemma 3. $\det \mathbf{B} = \delta \cdot \dfrac{\prod_{1 \le y < j \le q} (\mathsf{id}_y - \mathsf{id}_j) \prod_{1 \le i < k \le q+n+1} (\alpha_i - \alpha_k)}{\prod_{k=1}^{q+n+1} \prod_{y=1}^{q} (\alpha_k + \mathsf{id}_y)}$ *for constant* $\delta \in \mathbb{Z}_{p_2}^*$.

From Lemma 3 and the distinctness of $\mathsf{id}_1, \ldots, \mathsf{id}_q \bmod p_2$ (which is ensured since G_0), it is clear that $\det \mathbf{B} \neq 0$ as long as $\alpha_i \neq \alpha_j \bmod p_2$ for all $i, j \in [q+n+1]$, which happens with probability $> 1 - \frac{(q+n+1)^2}{p_2}$. In this case, we have $\det(\mathbf{A}) \neq 0 \bmod p_2$, so that the left-hand-side member of (1) is uniform over $\mathbb{Z}_{p_2}^{n+q+1}$. Therefore, $|\Pr[E_4] - \Pr[E_5]| \le (q+n+1)^2/p_2$.

G_6: In this game, challenge ciphertext is generated as

$$C_1^* \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1 p_2}, \qquad C_2^* = C_1^{*1/\tilde{\gamma}}, \qquad C_0^* = M_\beta \oplus K$$

where $K \xleftarrow{R} \{0,1\}^\rho$. In game G_5, we note that t_0 only appears in C_0^* and it is independent of $(U_i)_{i=1}^n$ and the keys obtained by $\mathscr{A}$. Letting $C_1^* = g^{s\gamma} \cdot g_2^{\omega_2}$ for some $\omega_2 \in_R \mathbb{Z}_{p_2}$, we have

$$\mathsf{H}(e(C_1^*, U_0)) = \mathsf{H}(e(g^{s\cdot\gamma}, u) \cdot e(g_2^{\omega_2}, g_2^{t_0})).$$

Conditionally on $\mathscr{A}$'s view, $e(C_1^*, U_0)$ has $\log(p_2)$ bits of min-entropy as long as C_1^* has a non-trivial $\mathbb{G}_{p_2}$ component. Since $\omega_2 \neq 0 \bmod p_2$ with probability $1-1/p_2$ and H is a universal hash function, the Leftover Hash Lemma ensures that $\mathsf{H}(e(C_1^*, U_0))$ is within distance at most $2^{-\lambda}$ from the uniform distribution over $\{0,1\}^\rho$. This implies that $|\Pr[E_5] - \Pr[E_6]| \leq 1/p_2 + 1/2^\lambda$. Since $\beta \in \{0,1\}$ is perfectly hidden from the adversary in G_6, we have $\Pr[E_6] = 1/2$.

Combining the above, $\mathscr{A}$'s advantage can be bounded as $\mathsf{Adv}^{\mathscr{A}}_{\mathcal{IBBE},\mathsf{sid\text{-}cpa}}(\lambda) = |\Pr[E_r] - \Pr[E_6]|$. □

4 Fuzzy IBE with Short Ciphertexts

We now present a fuzzy IBE scheme obtained by transposing the prime-order construction of Herranz *et al.* [37, 4] to composite order groups. The security of their scheme relies on the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) assumption. As in Section 3, we start with an explanation of why this assumption is not covered by the Uber assumption of [24].

Déjà Q framework does not cover aMSE-DDH assumption [37, 4]. Let an asymmetric prime-order pairing configuration $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. We describe an asymmetric version of the (ℓ, m, t)-aMSE-DDH assumption.[7] With a length-$(\ell+m)$ vector $\boldsymbol{y} = (y_1, \ldots, y_{l+m})$, define functions $f(Y) = \prod_{i=1}^{\ell}(Y + y_i)$ and $g(Y) = \prod_{i=\ell+1}^{\ell+m}(Y + y_i)$. Let g_0, h_0 be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ and pick $k, \gamma, \alpha, \beta \xleftarrow{R} \mathbb{Z}_p$. The (ℓ, m, t)-aMSE-DDH assumption states that given

$$\begin{array}{llll}
g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{\ell+t-2}}, & g_0^{k\gamma f(\gamma)}, & h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{m-2}}, & h_0^{kg(\gamma)}, \\
g_0^{\beta\gamma}, \ldots, g_0^{\beta\gamma^{\ell+t-2}}, & & h_0^{\beta}, h_0^{\beta\gamma}, \ldots, h_0^{\beta\gamma^{m-1}}, & \\
g_0^{\alpha}, g_0^{\alpha\gamma}, \ldots, g_0^{\alpha\gamma^{\ell+t}}, & & h_0^{\alpha}, h_0^{\alpha\gamma}, \ldots, h_0^{\alpha\gamma^{2(m-t)+3}}, &
\end{array}$$

and $T \in \mathbb{G}_T$, it is hard to determine whether $T = e(g_0, h_0)^{kf(\gamma)}$ or $T \in_R \mathbb{G}_T$.

We observe that the first line of the input is quite similar to the input of the GDDHE assumption [27] (cf. Section 3.1). We can transpose the discussion in Section 3.1 to the aMSE-DDH assumption. As we have shown, the gap between the uber assumption [24] and the aMSE-DDH assumption is due to the structures of polynomials in the exponents of h_0 and the entry $g_0^{k\gamma f(\gamma)}$ which shares $kf(\gamma)$ with the challenge. We therefore conclude that the Déjà Q framework [24] does not subsume the (ℓ, m, t)-aMSE-DDH assumption.

In this section as well, we are not going to start from the aMSE-DDH assumption. Instead, we will try to adapt Herranz *et al.*'s prime-order construction [37] into composite-order groups and analyse its selective security directly. Our fuzzy IBE scheme preserves the advantages of Herranz *et al.*'s [37] such as constant-size ciphertexts and can now be proved secure under static assumptions.

4.1 Construction

Before presenting the construction, we first describe the algorithm $\mathsf{Aggregate}$ of [28, 4].

[7] The assumption is originally given in symmetric groups. In order to work with the Déjà Q framework, one must transform it into asymmetric groups (using Abe *et al.*'s method [3] as suggested in [24]) which depends on the scheme and the reduction.

Aggregate Algorithm. The $\mathsf{Aggregate}$ algorithm of [28] was given for elements in $\mathbb{G}_T$, but it carries over to any prime order group [4]. Our construction requires it to work in composite order groups. Let a cyclic group $\mathbb{G}$ of composite order N. Given a set of pairs $\{u^{\frac{1}{\alpha+x_i}}, x_i\}_{i=1}^n$, where $u \in \mathbb{G}$ and $\alpha \in \mathbb{Z}_N$ are unknown and $x_1, \ldots, x_n \in \mathbb{Z}_N$ are pairwise distinct elements such that

$$\gcd(x_i - x_j, N) = 1 \quad \text{for all } i \neq j, \tag{2}$$

the algorithm computes the value $\mathsf{Aggregate}(\{u^{\frac{1}{\alpha+x_i}}, x_i\}_{i=1}^n) = u^{\frac{1}{\prod_{i=1}^n (\alpha+x_i)}}$ using $O(n^2)$ exponentiations. (See Appendix C for details.) It is unlikely to encounter a pair (x_i, x_j) violating restriction (2) since it exposes a non-trivial factorisation of N and violate the decisional subgroup assumption.

Our Fuzzy IBE Construction. In the description hereunder, we denote by n an upper bound on the number ℓ of attributes per identity. The construction goes as follows.

$\mathsf{Setup}(1^\lambda, 1^n)$**:** Choose $\rho \in \mathsf{poly}(\lambda)$ and define $\mathcal{M} = \{0,1\}^\rho$. Generate a composite-order pairing ensemble $(\mathcal{G} = (p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)) \longleftarrow \mathsf{GroupGen}(\rho + 2\lambda, 3)$ and set $N = p_1 p_2 p_3$. Then, arbitrarily select $n-1$ distinct dummy identities $d_1, \ldots, d_{n-1} \in \mathbb{Z}_N$. Define the set $\mathcal{I} = \mathbb{Z}_N \setminus \{d_1, \ldots, d_{n-1}\}$. Pick $g, u_0 \xleftarrow{\text{R}} \mathbb{G}_{p_1}$ and $g_3 \xleftarrow{\text{R}} \mathbb{G}_{p_3}$ and choose $\alpha, \gamma \xleftarrow{\text{R}} \mathbb{Z}_N$. Let $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$ be a universal hash function. Define $\mathsf{MSK} = (u_0, \alpha, \gamma, g_3)$ while the public parameters consist of

$$\mathsf{PP} = \big(\mathcal{G}_{\text{pub}},\ g,\ g^\gamma,\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ e(g,u_0)^\gamma,\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\big).$$

$\mathsf{KeyGen}(\mathsf{MSK}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\})$**:** Pick $u \xleftarrow{R} \mathbb{G}_{p_1}$, $X_{3,1}, \ldots, X_{3,\ell}$, $X'_{3,1}, \ldots, X'_{3,n-1}$, $X_{3,0} \xleftarrow{R} \mathbb{G}_{p_3}$ and output the secret key

$$\mathsf{SK}_S = \big(\ \big(K_i = u^{\frac{\gamma}{\alpha+\mathsf{id}_i}} \cdot X_{3,i}\big)_{i=1}^{\ell},\quad \big(K'_i = u^{\alpha^i} \cdot X'_{3,i}\big)_{i=1}^{n-1},\quad K_0 = u \cdot u_0 \cdot X_{3,0}\ \big).$$

$\mathsf{Encrypt}(\mathsf{PP}, S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}, \tau \leq \ell, M)$**:** To encrypt $M \in \{0,1\}^\rho$ for the set S with threshold τ, compute coefficients $\{c_j\}_{j \in [0, n+\tau-1]}$ for the polynomial

$$p_{S,\tau}(x) = \textstyle\prod_{i=1}^{\ell}(x + \mathsf{id}_i) \cdot \prod_{i=1}^{n+\tau-1-\ell}(x + d_i) = \sum_{i=0}^{n+\tau-1} c_i x^i \in \mathbb{Z}_N[x].$$

Choose $s \xleftarrow{\text{R}} \mathbb{Z}_N$ and output the ciphertext

$$\mathsf{CT}_{S,\tau} = \big(\ C_0 = M \oplus \mathsf{H}(e(g,u_0)^{s\gamma}),\quad C_1 = g^{s\gamma},\quad C_2 = \big(g^{c_0} \cdot \textstyle\prod_{i=1}^{n+\tau-1} G_i^{c_i}\big)^s = g^{s \cdot p_{S,\tau}(\alpha)}\ \big).$$

$\mathsf{Decrypt}(\mathsf{PP}, S, \tau, \mathsf{CT}, S', \mathsf{SK}_{S'})$**:** If $|S \cap S'| < \tau$, return $\perp$. Otherwise, we can find a set $\bar{S} \subseteq \mathcal{I}$ satisfying $\bar{S} \subseteq S \cap S'$ and $|\bar{S}| = \tau$. Note that the choice of $\bar{S}$ is arbitrary. By invoking algorithm $\mathsf{Aggregate}$, we can compute

$$K_{\mathsf{Agg}} = u^{\frac{\gamma}{\prod_{\mathsf{id} \in \bar{S}} (\alpha + \mathsf{id})}} \cdot X_{3,\mathsf{Agg}}$$

for some $X_{3,\mathsf{Agg}} \in \mathbb{G}_{p_3}$. Let

$$p_{S,\bar{S},\tau}(x) = p_{S,\tau}(x) / \textstyle\prod_{\mathsf{id} \in \bar{S}}(x + \mathsf{id}) = \sum_{i=0}^{n-1} z_i x^i$$

where $z_0 = \prod_{\mathsf{id} \in S \setminus \bar{S}} \mathsf{id} \cdot \prod_{i=1}^{n+\tau-1-|S|} d_i$. We can compute

$$\begin{aligned}
A_1 &= e(C_1, \textstyle\prod_{i=1}^{n-1}(K'_i)^{z_i}) = e(g^{s\gamma}, u^{p_{S,\bar{S},\tau}(\alpha) - z_0}) = e(g,u)^{s\gamma(p_{S,\bar{S},\tau}(\alpha) - z_0)},\\
A_2 &= e(C_2, K_{\mathsf{Agg}}) = e(g^{s \cdot p_{S,\tau}(\alpha)}, u^{\frac{\gamma}{\prod_{\mathsf{id} \in \bar{S}} (\alpha + \mathsf{id})}} \cdot X_{3,\mathsf{Agg}}) = e(g,u)^{s\gamma p_{S,\bar{S},\tau}(\alpha)},\\
A_3 &= e(C_1, K_0) = e(g^{s\gamma}, u \cdot u_0 \cdot X_{3,0}) = e(g,u)^{s\gamma} \cdot e(g,u_0)^{s\gamma},
\end{aligned}$$

and recover the message as $M = C_0 \oplus \mathsf{H}\big(A_3 / (A_2/A_1)^{1/z_0}\big)$.

The scheme is easily seen to be correct. We note that Decrypt can be optimized to consume only 2 pairing operations by recovering $e(g,u)^{s\gamma} = e(C_1, K_0 \cdot (\prod_{i=1}^{n-1}(K'_i)^{z_i})^{1/z_0})/e(C_2, K_{\mathsf{Agg}}^{1/z_0})$.

4.2 Proof of Security

Theorem 2. *For any adversary $\mathscr{A}$ attacking $\mathcal{FIBE}$ in the* sid-cpa *model making at most q key extraction queries, there exist algorithms $\mathscr{B}_1, \mathscr{B}_2$ such that*

$$\mathsf{Adv}^{\mathscr{A}}_{\mathcal{FIBE},\mathsf{sid\text{-}cpa}}(\lambda) \le 2 \cdot \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda) + (\ell+n+2) \cdot \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda) + \tfrac{q\cdot(\ell+2n)^2}{p_2} + \tfrac{1}{p_2} + \tfrac{1}{2^\lambda}.$$

where ℓ is maximum size of attribute sets.

Proof Sketch. Let $(S^* = (\mathsf{id}^*_1, \ldots, \mathsf{id}^*_{\ell^*}), \tau^*)$ be the challenge set and challenge threshold; $S_1, \ldots, S_q$ denote the sets provided in extract queries. It is worth noting that each secret key corresponds to an instance of our IBBE with its own random source u, denoted by $u_1, \ldots, u_q$ for $\mathsf{SK}_{S_1}, \ldots, \mathsf{SK}_{S_q}$, respectively. Following a game sequence analogous to that for IBBE (from G_r to G_4), we reach the following simulation strategy: the public parameters are

$$\left(\mathcal{G}_{\mathrm{pub}},\ g,\ \boxed{g^{\gamma}},\ \left(G_i = g^{\alpha^i}\right)_{i=1}^{2n-1},\ \boxed{e(g^{\gamma}, U_0)},\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\right)$$

where $\gamma = \tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha) \bmod N$ with $\tilde{\gamma} \xleftarrow{R} \mathbb{Z}_N$ and $U_0 = u_0 \cdot X_{3.0}$ with $X_{3,0} \xleftarrow{R} \mathbb{G}_{p_3}$. The challenge is

$$\left(C^*_1 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1p_2},\quad C^*_2 = {C^*_1}^{1/\tilde{\gamma}},\quad C^*_0 = M_\beta \oplus \mathsf{H}(e(C^*_1, U_0))\right);$$

a secret key for $S_y = \{\mathsf{id}_{1,y}, \ldots, \mathsf{id}_{\ell_y,y}\}$ $(y \in [q])$ consists of

$$\left(K_{i,y} = u_y^{\frac{\tilde{\gamma}\cdot p_{S^*,\tau^*}(\alpha)}{\alpha+\mathsf{id}_{i,y}}} \cdot \boxed{g_2^{\tilde{\gamma}\sum_{j=1}^{\ell_y+n} \frac{p_{S^*,\tau^*}(\alpha_j)}{\alpha_j+\mathsf{id}_{i,y}} r_{j,y}}} \cdot X_{3,i,y}\right)_{i=1}^{\ell_y},\ \left(K'_{i,y} = u_y^{\alpha^i} \cdot \boxed{g_2^{\sum_{j=1}^{\ell_y+n} \alpha_j^i r_{j,y}}} \cdot X'_{3,i,y}\right)_{i=1}^{n-1},$$

$$K_{0,y} = u_y \cdot \boxed{g_2^{\sum_{j=1}^{\ell_y+n} r_{j,y}}} \cdot U_0 \cdot X_{3,0,y},$$

where $\alpha, \alpha_1, \ldots, \alpha_{\ell+n} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are shared among all keys but $r_{1,y}, \ldots, r_{\ell+n,y} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are fresh.

As in the IBBE case, we want to claim that it is a (ℓ_y+n)-wise independent function that has been formed on the exponent of g_2 (in the boxed term). For each key, say SK_S with $S = \{\mathsf{id}_1, \ldots, \mathsf{id}_\ell\}$ for simplicity, it must hold that $\tau = |S \cap S^*| < \tau^*$ and we can assume $\mathsf{id}_1 = \mathsf{id}^*_1,\ \ldots,\ \mathsf{id}_\tau = \mathsf{id}^*_\tau$. This claim (w.r.t. SK_S) follows from the fact that the $(\ell+n) \times (\ell+n)$ matrix containing

$$\overbrace{\alpha^0 = 1}^{K_0},\quad \overbrace{\{\alpha^i\}_{i=1}^{n-1}}^{K'_i},\quad \overbrace{\left\{\prod_{\zeta\in[\tau]\setminus\{i\}} (\alpha+\mathsf{id}_\zeta) \cdot \prod_{\zeta=1}^{n+\tau-1-\ell} (\alpha+d_\zeta)\right\}_{i=1}^{\tau},\quad \left\{\frac{p_{S^*,\tau^*}(\alpha)}{\alpha+\mathsf{id}_i}\right\}_{i=\tau+1}^{\ell}}^{K_i}$$

for $\alpha \in \{\alpha_1, \ldots, \alpha_{\ell+n}\}$ has a non-zero determinant with high probability under the restriction $\tau < \tau^*$. This then implies that $K_{0,y}$ in SK_{S_y} $(y \in [q])$ will have a non-trivial $\mathbb{G}_{p_2}$ component independent of all other information, denoted by $\widehat{U}_y$.

Finally, we introduce a non-trivial $\mathbb{G}_{p_2}$ component into U_0 by the DS2 assumption, and argue that, conditioned on $e(g, U_0)$, $U_0 \cdot \widehat{U}_1$, $\ldots$, $U_0 \cdot \widehat{U}_q$, the $\mathbb{G}_{p_2}$ component of U_0 is still distributed uniformly. That is $e(C^*_1, U_0)$ has min-entropy of $\log(p_2)$ bits, and the leftover hash lemma ensures that the information about β will be statistically hidden. See Appendix D for more details. □

References

1. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In *Crypto'05*, *LNCS* 3621, 2005.
2. M. Abdalla, E. Kiltz, G. Neven. Generalized Key Delegation for Hierarchical Identity-Based Encryption. In *ESORICS'07*, *LNCS* 4734, 2007.
3. M. Abe, J. Groth, M. Ohkubo, and T. Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. *Crypto 2014*, LNCS 8616, 2014.
4. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, C. Ràfols. Attribute-based encryption schemes with constant-size ciphertexts. *Theor. Comput. Sci.* Volume 422, (2012).
5. N. Attrapadung, B. Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In *PKC 2010*, *LNCS* 6056, 2010.
6. N. Attrapadung, B. Libert, E. Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *PKC 2011*, *LNCS* 6571, 2011.
7. N. Attrapadung. Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More. In *Eurocrypt'14*, *LNCS* 8441, 2014.
8. M. Bellare, P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *1st ACM Conference on Computer and Communications Security*, 1993.
9. D. Boneh, X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Eurocrypt'04*, *LNCS* 3027, pp. 223–238. Springer-Verlag, 2004.
10. D. Boneh, X. Boyen, E.-J. Goh. Hierarchical Identity-Based encryption with Constant Size Ciphertext. In *Eurocrypt'05*, *LNCS* 3494, 2005.
11. D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano. Public Key Encryption with Keyword Search. In *Eurocrypt'04*, *LNCS* 3027, 2004.
12. D. Boneh, M. Franklin. Identity-Based Encryption from the Weil Pairing. In *SIAM* Journal of Computing 32(3), pp. 586–615, 2003, earlier version in *Crypto'01*, *LNCS* 2139, pp. 213–229, 2001.
13. D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, D. Vinayagamurthy. Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. In *Eurocrypt* 2014, *LNCS* 8441, 2014.
14. D. Boneh, C. Gentry and B. Waters. Collusion-Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In *Crypto'05*, *LNCS* 3621, 2005.
15. D. Boneh, M. Hamburg. Generalized Identity Based and Broadcast Encryption Schemes. In *Asiacrypt'08*, *LNCS* 5350, 2008.
16. D. Boneh, A. Sahai, B. Waters. Functional Encryption: Definitions and Challenges. In *TCC'11*, *LNCS* 6597, 2011.
17. D. Boneh, B. Waters, M. Zhandry. Low-overhead Broadcast Encryption from Multi-Linear Maps. In *Crypto'14*, *LNCS* 8616, 2014.
18. X. Boyen, B. Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In *Crypto'06*, *LNCS* 4117, 2006.
19. R. Canetti, S. Halevi, J. Katz. A Forward-Secure Public-Key Encryption Scheme. In *Eurocrypt'03*, *LNCS* 2656, 2003.
20. J. Chen, J. Gong, J. Weng. Tightly Secure IBE Under Constant-Size Master Public Key. In *PKC (1) 2017*, *LNCS* 10174, 2017.
21. J. Chen, B. Libert, S. Ramanna. Non-Zero Inner Product Encryption with Short Ciphertexts and Private Keys. In *SCN 2016*, *LNCS* 9841, pp. 23–41, 2016.
22. J. Chen, H. Wee. Semi-Adaptive Attribute-Based Encryption and Improved Delegation for Boolean Formula In *SCN 2014*, *LNCS* 8642, 2014.
23. M. Chase, S. Meiklejohn. Déjà Q: Using Dual Systems to Revisit q-Type Assumptions. In *Eurocrypt 2014*, *LNCS* 8441, 2014.
24. M. Chase, M. Maller, S. Meiklejohn. Déjà Q All Over Again: Tighter and Broader Reductions of q-Type Assumptions. In *Asiacrypt (2) 2016*, *LNCS* 10032, 2016.
25. J.-H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In *Eurocrypt'06*, *LNCS* 4004, 2006.
26. J.-H. Cheon, K. Han, C. Lee, H. Ryu. D. Stehlé. Cryptanalysis of the Multilinear Map over the Integers. In *Eurocrypt'15*, *LNCS* 9056, 2015.
27. C. Delerablée. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In *Asiacrypt 2007*, *LNCS* 4833, 2007.

28. C. Delerablée, D. Pointcheval. Dynamic Threshold Public-Key Encryption. In *Crypto 2008*, *LNCS* 5157, 2007.
29. D. Derler, T. Jager, D. Slamanig, C. Striecks. Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange. In *Eurocrypt 2018*, *LNCS* 10822, 2018.
30. A. Fiat, M. Naor. Broadcast Encryption. In *Crypto'93*, *LNCS* 773, 1993.
31. D. Freeman. Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups. In *Eurocrypt'10*, *LNCS* 6110, 2010.
32. R. Gay, I. Kerenidis, H. Wee. Communication Complexity of Conditional Disclosure of Secrets and Attribute-Based Encryption. In *Crypto'15*, *LNCS* 9216, 2015.
33. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, B. Waters. Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. *FOCS 2013*, 2013
34. C. Gentry, B. Waters. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In *Eurocrypt'09*, *LNCS* 5479, 2009.
35. S. Gorbunov, V. Vaikuntanathan, H. Wee. Attribute-Based Encryption for Circuits from LWE. In *STOC 2013*, 2013.
36. V. Goyal, O. Pandey, A. Sahai, B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS'06*, 2006.
37. J. Herranz, F. Laguillaumie, C. Ràfols. Constant-Size Ciphertexts in Threshold Attribute-Based Encryption. In *PKC'10*, *LNCS* 6056, 2010.
38. S. Hohenberger, B. Waters. Attribute-Based Encryption with Fast Decryption. In *PKC 2013*, *LNCS* 7778, 2013.
39. J. Katz, Y. Lindell. Introduction to Modern Cryptography, Second Edition. Chapman and Hall/CRC 2008.
40. J. Katz, A. Sahai, B. Waters. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. In *Eurocrypt'08*, *LNCS* 4965, 2008.
41. A. Lewko, A. Sahai, and B. Waters. Revocation Systems with Very Small Private Keys. In *IEEE Symposium on Security and Privacy, 2010*, 2010.
42. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In *Eurocrypt 2010*, *LNCS* 6110, 2010.
43. A. Lewko, B. Waters. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts. In *TCC 2010*, LNCS 5978, 2010.
44. M. Naor, D. Naor, J. Lotspiech. Revocation and Tracing Schemes for Stateless Receivers. In *Crypto 2001*, LNCS 2139, 2001.
45. M. Naor, B. Pinkas. Efficient Trace and Revoke Schemes. In *Financial Cryptography 2000*, *LNCS* 1962, 2000.
46. L. Nguyen. Accumulators from Bilinear Pairings and Applications. In *CT-RSA'05*, *LNCS* 3376, 2005.
47. T. Okamoto, K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Crypto'10*, *LNCS* 6223, 2010.
48. T. Okamoto, K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In *CANS 2011*, *LNCS* 7092, 2011.
49. T. Okamoto, K. Takashima. Fully Secure Unbounded Inner-Product and Attribute-Based Encryption. In *Asiacrypt'12*, *LNCS* 7658, 2012.
50. T. Okamoto, K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. Designs, Codes and Cryptography 77.2-3 (2015): 725–771.
51. R. Ostrovsky, A. Sahai, B. Waters. Attribute-based encryption with non-monotonic access structures. In *ACM CCS'07*, 2007.
52. Y. Rouselakis, B. Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In *ACM CCCS 2013*, 2013.
53. R. Sakai, J. Furukawa. Identity-Based Broadcast Encryption. In Cryptology ePrint Archive: Report 2007/217, `http://eprint.iacr.org/2007/217`, 2007.
54. R. Sakai, M. Kasahara. ID-based Cryptosystems with Pairing on Elliptic Curve. In Cryptology ePrint Archive: Report 2003/054, `http://eprint.iacr.org/2003/054`, 2003.
55. A. Sahai, B. Waters. Fuzzy Identity-Based Encryption In *Eurocrypt'05*, *LNCS* 3494, 2005.
56. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Crypto'84*, *LNCS* 196, 1984.
57. K. Takashima. Expressive Attribute-Based Encryption with Constant-Size Ciphertexts from the Decisional Linear Assumption. In *SCN 2014*, *LNCS* 8642, 2014.
58. K. Takashima. New Proof Techniques for DLIN-Based Adaptively Secure Attribute-Based Encryption. In *ACISP 2017*, LNCS, to appear, 2017.
59. B. Waters. Efficient Identity-Based Encryption without Random Oracles. In *Eurocrypt 2005*, *LNCS* 3494. 2005.
60. B. Waters. Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. In *Crypto 2009*, *LNCS* 5677. 2009.

61. B. Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In *PKC 2011*, *LNCS* 6571. 2011.
62. B. Waters. Functional Encryption for Regular Languages. In *Crypto 2012*, *LNCS* 7417. 2012.
63. H. Wee. Déjà Q Encore! Un petit IBE. In *TCC 2016*, *LNCS* 9563, 2016.

A Comparisons with Prior Works

We give detailed comparisons between our two schemes and earlier realizations along with more discussions.

Table 1 provides a detailed comparison between our IBBE system and other IBBE with short ciphertexts and secret keys. Table 2 compares our FIBE with previous FIBE with short ciphertexts. We fix the following notation: CT: ciphertext; $\mathsf{SK}_{\mathsf{id}}$: secret key for identity id; #dec: cost of decryption; ρ is the length of the message to be encrypted; $\mathbb{G}_N$: symmetric pairing group with order N (a composite number); $\mathbb{G}_1$, $\mathbb{G}_2$: source groups of an asymmetric prime-order pairing of order p, a prime; [P]: a pairing operation; [M]: scalar multiplication in the source groups; aID: adaptive/full security; sID: security selective identity model; na-sID: security in the selective model with non-adaptive key extraction queries; saID: security in semi-adaptive model; GDDHE: generalised decision Diffie-Hellman exponent assumption; O-GDDHE: an oracle variant of GDDHE; GGM: proven secure in the generic (bilinear) group model; aMSE-DDH: augmented multi-sequence of exponents decisional Diffie-Hellman assumption; Static: standard assumption in composite-order pairing group, such as subgroup decision assumption and subgroup Diffie-Hellman assumption.

IBBE	$\lvert\mathsf{CT}\rvert$	$\lvert\mathsf{SK}_{\mathsf{id}}\rvert$	#dec	Security	Assumption	RO
[27]-1	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + \rho$	$\lvert\mathbb{G}_1\rvert$	2[P]+$O(n)$[M]	sID	GDDHE	Yes
[27]-2[8]	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + \rho$	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{Z}_p\rvert$	2[P]+$O(n)$[M]	na-sID	O-GDDHE	No
[53]	$2\lvert\mathbb{G}_1\rvert + \rho$	$\lvert\mathbb{G}_2\rvert$	2[P]+$O(n)$[M]	aID	GGM	Yes
Ours	$2\lvert\mathbb{G}_N\rvert + \rho$	$\lvert\mathbb{G}_N\rvert$	2[P]+$O(n)$[M]	sID	Static	No

Table 1. Comparison among compact IBBE (with short ciphertexts and secret keys). Here, n is the maximum number of recipients.

FIBE	$\lvert\mathsf{CT}\rvert$	$\lvert\mathsf{SK}_{\mathsf{id}}\rvert$	#dec	Security	Assumption
[37]	$2\lvert\mathbb{G}_1\rvert + \rho$	$n\lvert\mathbb{G}_1\rvert + n\lvert\mathbb{G}_2\rvert$	2[P] + $O(\tau^2 + n)$[M]	sID	aMSE-DDH
[6],[4]	$2\lvert\mathbb{G}_1\rvert + \rho$	$(n^2 + n)\lvert\mathbb{G}_2\rvert$	2[P] + $O(n\tau)$[M]	sID	DBDHE
[22]	$2\lvert\mathbb{G}_N\rvert + \rho$	$(n^2 + n)\lvert\mathbb{G}_N\rvert$	2[P] + $O(n\tau)$[M]	saID	Static
[57]	$17\lvert\mathbb{G}_1\rvert + \rho$	$(6n^2 + 5)\lvert\mathbb{G}_2\rvert$	17[P] + $O(n\tau)$[M]	saID	DLIN
[7]	$6\lvert\mathbb{G}_1\rvert + \rho$	$(n^2 + 2n + 3)\lvert\mathbb{G}_2\rvert$	6[P] + $O(n\tau)$[M]	aID	Static
Ours	$2\lvert\mathbb{G}_N\rvert + \rho$	$2n\lvert\mathbb{G}_N\rvert$	2[P] + $O(\tau^2 + n)$[M]	sID	Static

Table 2. Comparison among compact FIBE. Here n is the (maximum) size of attribute set and τ is the threshold.

[8] The parameters provided here are only based on the claims made in [27]. It is claimed that there are two possible ways to remove the random oracles – one is to randomise the keys and the other is to use an oracle variant of GDDHE, without a proof for the latter. Furthermore, it is not clear how the construction obtained by randomising the keys (similar to the IBE of [9]) really works, since the ciphertexts in the broadcast setting are structurally different from those of the IBE.

Although composite order groups are known to have less efficient implementations than prime order bilinear groups, we feel that using the former for our constructions is justified. There is a clear asymptotic efficiency benefit over existing constructions (e.g., [15]) achieving comparable security guarantees. In both schemes, the number of pairing evaluations is constant. Indeed, a product of two pairings (which is significantly faster to compute than two independent pairings) suffices to decrypt whereas the encryption algorithm does not require any pairing evaluation at all. In the FIBE case, we go from quadratic to linear key sizes in the maximal number of attributes per ciphertext when we compare it to, e.g., [6]. In the IBBE case, we get constant-size ciphertexts and keys for the first time under constant-size assumptions.

When the underlying assumptions are taken into account, the benefit of composite order groups becomes even clearer as we only rely on well-established assumptions whereas the prime order variants [27, 37] of our schemes require completely *ad hoc* assumptions that are not even easy to memorise. We believe the longer the description of an assumption is, the more it looks like another way to state that the scheme is insecure. The following statement from [39] (p25) buttresses our belief: *"...there is a general preference for assumptions that are simpler to state, since such assumptions are easier to study and to refute."*.

We further remark that the security loss of both our schemes is proportional to the maximum size of the sets associated with ciphertexts or than the number of key extraction queries, whichever is higher. Furthermore we emphasize that a reduction to a standard assumption with some security loss is more reasonable than a tight reduction to an ad-hoc parameterized assumption since the actual strength of a parameterized assumption is typically questionable [25].

B Deferred Proofs for the IBBE System

Proofs of Lemmas

Proof (of Lemma 1). The reduction $\mathscr{B}_1$ receives an instance $(\mathcal{G}_{\mathrm{pub}}, g_1, g_3, T)$ of DS1 and simulates the $\mathsf{sid\text{-}cpa}$ game to $\mathscr{A}$ as follows.

Setup. The adversary $\mathscr{A}$ commits to the challenge identity set $S^* = \{\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*\}$. Algorithm $\mathscr{B}_1$ samples $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and sets $\gamma = \tilde{\gamma} \cdot p_{S^*}(\alpha)$. It sets $g = g_1$, chooses $u \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ and further computes $G_i = g^{\alpha^i}$ $U_i = u^{\alpha^i} \cdot R_{3,i}$ for $i \in [n]$. Sampling from $\mathbb{G}_{p_1}$ and $\mathbb{G}_{p_3}$ is done using g_1 and g_3, respectively. $\mathscr{B}_1$ chooses $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$, a universal hash function and provides the following public parameters to $\mathscr{A}$.

$$\mathsf{PP} = (\mathcal{G}_{\mathrm{pub}},\ g,\ g^\gamma,\ (G_i = g^{\alpha^i},\ U_i = u^{\alpha^i} \cdot R_{3,i})_{i=1}^n,\ e(g,u)^\gamma,\ \mathsf{H}).$$

Key Extraction Phase. Upon a key extraction query on id_y, $\mathscr{B}_1$ picks $X_{3,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ and responds with

$$\mathsf{SK}_{\mathsf{id}_y} = u^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot X_{3,y}.$$

In the challenge phase, $\mathscr{A}$ provides two messages $M_0, M_1 \in \{0,1\}^\rho$.

Challenge. The reduction algorithm picks a random bit $\beta \xleftarrow{\mathrm{R}} \{0,1\}$ and sets $C_1^* = T$, $C_2^* = (C_1^*)^{1/\tilde{\gamma}}$ and $C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0))$; sends $\mathsf{CT}^* = (C_0^*, C_1^*, C_2^*)$ to $\mathscr{A}$.

Guess. At the end of the game, $\mathscr{A}$ returns its guess β' and $\mathscr{B}_1$ returns 1 if and only if $\beta = \beta'$.

Observe that the distribution of CT^* is as in game G_2 if $T \in \mathbb{G}_{p_1}$ and identical to G_3 if $T \in \mathbb{G}_{p_1 p_2}$. This readily proves the lemma. □

Proof (of Lemma 2). On input an instance $(\mathcal{G}_{\mathrm{pub}}, g_1, g_3, h_{12}, h_{23}, T)$ of DS2 problem, the reduction $\mathscr{B}_2$ simulates the $\mathsf{sid\text{-}cpa}$ game as follows.

Setup. Once $\mathscr{A}$ commits to the identity set $S^* = \{\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*\}$, $\mathscr{B}_2$ chooses $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$, sets $\gamma = \tilde{\gamma} \cdot p_{S^*}(\alpha)$, $g = g_1$ and computes $G_i = g^{\alpha^i}$ for each $i \in [n]$. It then chooses $\{r'_j, \alpha_j\}_{j=1}^{k-1} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and generates $\{U_i\}_{i=0}^n$ as

$$U_i = T^{\alpha^i} \cdot h_{23}^{\sum_{j=1}^{k-1} r'_j \alpha_j^i} \cdot R'_{3,i} \qquad \forall i \in \{0, \ldots, n\},$$

where $R'_{3,i} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. It provides the adversary with public parameters

$$\mathsf{PP} = (\mathcal{G}_{\mathrm{pub}},\ g,\ g^{\gamma},\ (G_i = g^{\alpha^i},\ U_i = u^{\alpha^i} \cdot R_{3,i})_{i=1}^n,\ e(g,u)^{\gamma},\ \mathsf{H}),$$

where $e(g,u)^{\gamma}$ is computed as $e(g, U_0)^{\gamma}$, which has the proper distribution.

Key Extraction Phase. For a private key query on id_y for $y \in [q]$, a secret key is produced as

$$\mathsf{SK}_{\mathsf{id}_y} = T^{\frac{\tilde{\gamma} \cdot p_{S^*}(\alpha)}{\alpha + \mathsf{id}_y}} \cdot h_{23}^{\sum_{j=1}^{k-1} \frac{r'_j \cdot \tilde{\gamma} \cdot p_{S^*}(\alpha_j)}{\alpha_j + \mathsf{id}_y}} \cdot X'_{3,y},$$

where $X'_{3,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. Writing $h_{23} = g_2^t \cdot h_3$ with $t \in \mathbb{Z}_{p_2}^*$ and $h_3 \in \mathbb{G}_{p_3}$, we have $r_j = t r'_j \bmod p_2$ for $j \in [q + n + 1]$, which is distributed uniformly over $\mathbb{Z}_{p_2}$, as required. Also, we observe that

$$R_{3,i} = R'_{3,i} \cdot h_3^{\sum_{j=1}^{k-1} r'_j \alpha_j^i} \qquad \text{and} \qquad X_{3,y} = X'_{3,y} \cdot h_3^{\sum_{j=1}^{k-1} \frac{r'_j \tilde{\gamma} \cdot p_{S^*}(\alpha_j)}{\alpha_j + \mathsf{id}_y}}$$

have the correct distribution in $\mathbb{G}_{p_3}$.

Challenge. In the challenge phase, $\mathscr{A}$ provides two messages $M_0, M_1 \in \{0,1\}^{\rho}$. At this point, $\mathscr{B}_2$ picks $\beta \xleftarrow{\mathrm{R}} \{0,1\}^n$, computes challenge ciphertext as

$$C_1^* = h_{12}, \qquad C_2^* = (C_1^*)^{1/\tilde{\gamma}}, \qquad C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0))$$

and sends $\mathsf{CT}^* = (C_0^*, C_1^*, C_2^*)$ to $\mathscr{A}$.

Guess. $\mathscr{A}$ guesses $\beta' \in \{0,1\}$ of β and $\mathscr{B}_2$ returns 1 if and only if $\beta = \beta'$.

The distribution of CT^* is identical to that in game $\mathsf{G}_{4.(k-1).1}$ if $T \in \mathbb{G}_{p_1 p_3}$ and as in $\mathsf{G}_{4.k.0}$ if $T \in \mathbb{G}_{p_1 p_2 p_3}$. This immediately proves the lemma. □

Proof (of Lemma 3). We want to show that

$$\left(\prod_{k=1}^{q+n+1} \prod_{y=1}^{q} (\alpha_k + \mathsf{id}_y) \right) \cdot \det \mathbf{B} = \left(\prod_{1 \le y < j \le q} (\mathsf{id}_y - \mathsf{id}_j) \right) \left(\prod_{1 \le i < k \le q+n+1} (\alpha_i - \alpha_k) \right),$$

where $\mathbf{B}$ is the $(q+n+1) \times (q+n+1)$ matrix given by

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q+n+1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{q+n+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_{q+n+1}^n \\ \frac{1}{\alpha_1 + \mathsf{id}_1} & \frac{1}{\alpha_2 + \mathsf{id}_1} & \cdots & \frac{1}{\alpha_{q+n+1} + \mathsf{id}_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_1 + \mathsf{id}_q} & \frac{1}{\alpha_2 + \mathsf{id}_q} & \cdots & \frac{1}{\alpha_{q+n+1} + \mathsf{id}_q} \end{pmatrix}.$$

Multiplying $\det \mathbf{B}$ by $\prod_{k=1}^{q+n+1} \prod_{y=1}^{q} (\alpha_k + \mathsf{id}_y)$ results in a sum $\mathcal{P}$ of homogeneous polynomials of degree

$$\frac{n(n+1)}{2} + q(q+n+1) - q = \frac{n(n+1)}{2} + q(q+n).$$

We note that $\det \mathbf{B}$ vanishes if

- $\alpha_i = \alpha_j$ for some $i, j \in [q+n+1]$ and columns i, j become identical.
- rows i, j (for some $i, j \in [n+2, q+n+1]$) become equal which happens when $\mathsf{id}_i = \mathsf{id}_j \bmod p_2$.

From these observations, it follows that $\mathcal{P}$ must be a multiple of $\mathcal{Q} = \prod_{1 \le y < j \le q} (\mathsf{id}_y - \mathsf{id}_j) \prod_{1 \le i < k \le q+n+1} (\alpha_i - \alpha_k)$. We have

$$\deg \mathcal{Q} = \frac{q(q-1)}{2} + \frac{(q+n+1)(q+n)}{2} = \frac{n(n+1)}{2} + q(q+n)$$

which happens to be equal to $\deg \mathcal{P}$. Therefore, $\mathcal{P}$ must be a constant multiple of $\mathcal{Q}$ from which the statement of the lemma follows. □

C Description of Aggregate algorithm

We describe the detail of Aggregate algorithm: Define $\Lambda_{0,\eta} = u^{1/(\alpha + x_\eta)}$ for each $\eta \in [n]$ and observe that, if we define

$$\Lambda_{j,\eta} = u^{\frac{1}{(\alpha+x_\eta) \cdot \prod_{i=1}^{j} (\alpha + x_i)}} \qquad \text{with} \quad 1 \le j < \eta \le n,$$

these values satisfy the formula

$$\Lambda_{j,\eta} = \Big(\frac{\Lambda_{j-1,j}}{\Lambda_{j-1,\eta}} \Big)^{1/(x_\eta - x_j)}. \tag{3}$$

As long as the distinct scalars $x_1, \ldots, x_n$ satisfy the condition (2), relation (3) allows sequentially computing $\Lambda_{j,\eta}$ for $j = 1$ to $n-1$ and $\eta = j+1$ to n and finally obtains $\Lambda_{n-1,n} = u^{\frac{1}{\prod_{i=1}^{n} (\alpha + x_i)}}$.

D Proof of Theorem 2

Proof. We prove the theorem via a game sequence. As usual we let $E_\square$ denote the event that $\mathscr{A}$ wins in $\mathsf{G}_\square$. Furthermore, we let (1) $(S^* = (\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*), \tau^*)$ be the challenge set and challenge threshold; (2) (M_0, M_1) be the challenge message pair; (3) $S_1, \ldots, S_q$ denote the sets provided in extract queries. We define $\ell = \max\{|S_1|, \ldots, |S_q|\}$ and describe the game sequence as follows.

G_r: This is the real security game.

G_0: This game is like G_r with the following modifications regarding the identities belonging to the set $S = S_1 \cup \cdots \cup S_q$: (1) No two distinct identities $\mathsf{id} \neq \mathsf{id}'$ mod N in S satisfy $\mathsf{id} \equiv \mathsf{id}' \bmod p_2$; (2) No identity $\mathsf{id} \in S$ satisfies $\alpha + \mathsf{id} \equiv 0 \bmod p_1$. By the argument in Section 3.3, we have

$$|\Pr[E_r] - \Pr[E_0]| \le \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda) + \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda).$$

G_1: This game is identical to G_0 except that, in the initialisation phase, we pick $\tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and define $\gamma = \tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha) \bmod N$. This change is conceptual and $\Pr[E_0] = \Pr[E_1]$. We note that γ can be explicitly computed. The master public key is

$$\mathsf{PP} = \Big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^{\gamma},\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ e(g,u_0)^{\gamma},\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\Big);$$

upon a query on $S_y = (\mathsf{id}_{1,y}, \ldots, \mathsf{id}_{\ell_y,y})$ $(y \in [q])$, the corresponding secret key SK_{S_y} is generated as

$$\big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot X_{3,i,y}\big)_{i=1}^{\ell_y},\ \big(K'_{i,y} = u_y^{\alpha^i} \cdot X'_{3,i,y}\big)_{i=1}^{n-1},\ K_{0,y} = u_y \cdot u_0 \cdot X_{3,0,y},$$

where $u_y \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ and $X_{3,1,y}, \ldots, X_{3,\ell_y,y}, X'_{3,1,y}, \ldots, X'_{3,n-1,y}, X_{3,0,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$; the challenge ciphertext is

$$C_0 = M_\beta \oplus \mathsf{H}(e(g,u_0)^{s\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}), \quad C_1 = g^{s\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}, \quad C_2 = g^{s \cdot p_{S^*,\tau^*}(\alpha)}.$$

where $\beta \xleftarrow{\mathrm{R}} \{0,1\}$ and $s \xleftarrow{\mathrm{R}} \mathbb{Z}_N$.

G_2: In this game, the public parameters are

$$\mathsf{PP} = \Big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^{\gamma},\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ \boxed{e(g,U_0)^{\gamma}},\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\Big);$$

where $U_0 = u_0 \cdot X_{3.0}$ with $X_{3,0} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$; the challenge ciphertext is generated as follows

$$C_1^* \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}, \qquad C_2^* = C_1^{*1/\tilde{\gamma}}, \qquad C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0)),$$

while the secret key SK_{S_y} for S_y is

$$\big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot X_{3,i,y}\big)_{i=1}^{\ell_y}, \qquad \big(K'_{i,y} = u_y^{\alpha^i} \cdot X'_{3,i,y}\big)_{i=1}^{n-1},$$

$$\boxed{K_{0,y} = u_y \cdot U_0 \cdot X_{3,0,y}}$$

Since $e(g,U_0) = e(g,u_0)$, we do not change the distribution of the public parameters. Following the reasoning in Section 3.3, we know that the modification here won't change the distribution of the challenge ciphertext. The change on $K_{0,y}$ will not change its distribution either due to the fresh randomness $X_{3,0,y}$ in each key. Thus, we have $\Pr[E_1] = \Pr[E_2]$.

G_3: This game is identical to G_2 except that the challenge ciphertext is created by first sampling $C_1^* \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1 p_2}$ rather than $C_1^* \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ and computing C_2^* and C_0^* as in G_2. As in Section 3.3, we can prove the following lemma.

Lemma 4. *There is a PPT algorithm $\mathscr{B}_1$ such that*

$$|\Pr[E_2] - \Pr[E_3]| \leq \mathsf{Adv}^{\mathscr{B}_1}_{\mathcal{G},\mathrm{DS1}}(\lambda).$$

G_4: We change the distribution of secret keys $\mathsf{SK}_{S_1}, \ldots, \mathsf{SK}_{S_q}$ by gradually introducing $\mathbb{G}_{p_2}$ components. To do so, we need the help of two sub-games $\mathsf{G}_{4.k.0}$, $\mathsf{G}_{4.k.1}$ defined as follows. Recall that $\ell = \max\{|S_1|, \ldots, |S_q|\}$ which ensures that each secret key has adequate randomness in $\mathbb{G}_{p_2}$ for the future argument. As before, we define $\mathsf{G}_{4.0.1} = \mathsf{G}_3$ and $\mathsf{G}_{4.\ell+n.1} = \mathsf{G}_4$.

– In $\mathsf{G}_{4.k.0}$ ($k \in [\ell + n]$), secret key SK_{S_y} for S_y ($y \in [q]$) such that $k \leq \ell_y + n$ is

$$\Big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot \boxed{g_2^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}} r_{k,y}}} \cdot g_2^{\tilde{\gamma} \sum_{j=1}^{k-1} \frac{p_{S^*,\tau^*}(\alpha_j)}{\alpha_j + \mathsf{id}_{i,y}} r_{j,y}} \cdot X_{3,i,y}\Big)_{i=1}^{\ell_y},$$
$$\Big(K'_{i,y} = u_y^{\alpha^i} \cdot \boxed{g_2^{\alpha^i r_{k,y}}} \cdot g_2^{\sum_{j=1}^{k-1} \alpha_j^i r_{j,y}} \cdot X'_{3,i,y}\Big)_{i=1}^{n-1},$$
$$K_{0,y} = u_y \cdot \boxed{g_2^{r_{k,y}}} \cdot g_2^{\sum_{j=1}^{k-1} r_{j,y}} \cdot U_0 \cdot X_{3,0,y},$$

where $g_2 \xleftarrow{\mathrm{R}} G_{p_2}$ is a generator of G_{p_2} and $r_{1,y}, \ldots, r_{k,y} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are fresh for each secret key. However we note that $\alpha_1, \ldots, \alpha_{k-1} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are shared among all secret keys. For the other case (i.e., $k > \ell_y + n$), the secret key is defined as in $\mathsf{G}_{4.k-1.1}$.

– In $\mathsf{G}_{4.k.1}$ ($k \in [0, \ell + n]$), a secret key SK_{S_y} for S_y ($y \in [q]$) is

$$\Big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot \boxed{g_2^{\tilde{\gamma} \sum_{j=1}^{k_y} \frac{p_{S^*,\tau^*}(\alpha_j)}{\alpha_j + \mathsf{id}_{i,y}} r_{j,y}}} \cdot X_{3,i,y}\Big)_{i=1}^{\ell_y},$$
$$\Big(K'_{i,y} = u_y^{\alpha^i} \cdot \boxed{g_2^{\sum_{j=1}^{k_y} \alpha_j^i r_{j,y}}} \cdot X'_{3,i,y}\Big)_{i=1}^{n-1},$$
$$K_{0,y} = u_y \cdot \boxed{g_2^{\sum_{j=1}^{k_y} r_{j,y}}} \cdot U_0 \cdot X_{3,0,y},$$

where $k_y = \min\{k, \ell_y + n\}$, $\alpha, \alpha_1, \ldots, \alpha_k \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are shared among all secret keys and $r_{1,y}, \ldots, r_{k_y,y} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ are fresh for each secret key.

By a similar argument in Section 3.3, we know that $\alpha \bmod p_2$ is only leaked from $\mathsf{SK}_{S_1}, \ldots, \mathsf{SK}_{S_q}$ in $\mathsf{G}_{4.k.0}$ and the CRT thus implies $\Pr[E_{4.k.0}] = \Pr[E_{4.k.1}]$ for all k. We also have the following lemma for all $k \in [\ell + n]$.

Lemma 5. *There exists a PPT algorithm $\mathscr{B}_2$ such that*

$$|\Pr[E_{4.(k-1).1}] - \Pr[E_{4.k.0}]| \leq \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda).$$

G_5**:** We replace the exponents in the $\mathbb{G}_{p_2}$-components of SK_{S_y} ($y \in [q]$) with independent random elements $t_{0,y}, t'_{1,y} \ldots, t'_{n-1,y}, t_{1,y}, \ldots, t_{\ell_y,y} \in \mathbb{Z}_N$. In particular, a private key SK_{S_y} for S_y ($y \in [q]$) is computed as

$$\Big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot \boxed{g_2^{t_{i,y}}} \cdot X_{3,i,y}\Big)_{i=1}^{\ell_y}, \ \Big(K'_{i,y} = u_y^{\alpha^i} \cdot \boxed{g_2^{t'_{i,y}}} \cdot X'_{3,i,y}\Big)_{i=1}^{n-1},$$

$$K_{0,y} = u_y \cdot \boxed{g_2^{t_{0,y}}} \cdot U_0 \cdot X_{3,0,y}$$

We are going to prove that G_5 and G_4 are statistically indistinguishable. For $y \in [q]$, we let the $\mathbb{G}_{p_2}$ component of $K_{0,y}$, $K'_{1,y}, \ldots, K'_{n-1,y}$, $K_{1,y}, \ldots, K_{\ell_y,y}$ in G_4 have logarithms

$\hat{t}_{0,y}, \hat{t}'_{1,y}, \ldots, \hat{t}'_{n-1,y}, \hat{t}_{1,y}, \ldots, \hat{t}_{\ell_y,y}$. With the notations

$$\mathbf{B}_y = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{\ell_y+n} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{\ell_y+n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_{\ell_y+n}^{n-1} \\ \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_1)}{\alpha_1+\mathsf{id}_{1,y}} & \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_2)}{\alpha_2+\mathsf{id}_{1,y}} & \cdots & \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_{\ell_y+n})}{\alpha_{\ell_y+n}+\mathsf{id}_{1,y}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_1)}{\alpha_1+\mathsf{id}_{\ell_y,y}} & \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_2)}{\alpha_2+\mathsf{id}_{\ell_y,y}} & \cdots & \frac{\tilde{\gamma} p_{S^*,\tau^*}(\alpha_{\ell_y+n})}{\alpha_{\ell_y+n}+\mathsf{id}_{\ell_y,y}} \end{pmatrix}$$

and

$$\mathbf{r}_y = (r_{1,y}, \ldots, r_{\ell_y+n,y})^\top \in \mathbb{Z}_N^{\ell_y+n},$$
$$\hat{\mathbf{t}}_y = (\hat{t}_{0,y}, \hat{t}'_{1,y}, \ldots, \hat{t}'_{n-1,y}, \hat{t}_{1,y}, \ldots, \hat{t}_{\ell_y,y})^\top \in \mathbb{Z}_N^{\ell_y+n},$$

we have

$$\begin{pmatrix} \hat{\mathbf{t}}_1 \\ \hat{\mathbf{t}}_2 \\ \vdots \\ \hat{\mathbf{t}}_q \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{B}_1 & & & \\ & \mathbf{B}_2 & & \\ & & \ddots & \\ & & & \mathbf{B}_q \end{pmatrix}}_{\mathbf{A}} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \vdots \\ \mathbf{r}_q \end{pmatrix}$$

The special structure of matrix $\mathbf{A}$ and the following lemma imply that all $\hat{\mathbf{t}}_y$ are uniform over $\mathbb{Z}_{p_2}^{\ell_y+n}$ with probability $1 - q(\ell+2n)^2/p_2$ and thus $|\Pr[E_4] - \Pr[E_5]| \leq q(\ell+2n)^2/p_2$.

Lemma 6. *The matrices $\mathbf{B}_1, \ldots, \mathbf{B}_q$ are all invertible with overwhelming probability $1-q(\ell+2n)^2/p_2$.*

Compare with the matrix $\mathbf{A}$ in Equation (1), the matrices $\mathbf{B}_1, \ldots, \mathbf{B}_q$ here are more complicated in the sense that, for each $y \in [q]$, there can be an $\mathsf{id} \in S_y$ such that $\frac{\tilde{\gamma} p_{S^*,\tau^*}(x)}{x+\mathsf{id}}$ is a polynomial in x, i.e., $\mathsf{id} \in S^*$. We can prove that when the number of such identities does not reach τ^* for each $y \in [q]$, all matrices $\mathbf{B}_1, \ldots, \mathbf{B}_q$ are still invertible with overwhelming probability.

G_6: In this game, we change the distribution of U_0 as follows.

$$U_0 = u_0 \cdot X_{3.0} \quad \longrightarrow \quad U_0 = u_0 \cdot g_2^{t_0} \cdot X_{3.0}.$$

where $t_0 \xleftarrow{\mathrm{R}} \mathbb{Z}_N$. This changes the distributions of both secret keys and challenge ciphertext. We have the following lemma.

Lemma 7. *There exists a PPT algorithm $\mathscr{B}_2$ such that we have the inequality $|\Pr[E_5] - \Pr[E_6]| \leq \mathsf{Adv}^{\mathscr{B}_2}_{\mathcal{G},\mathrm{DS2}}(\lambda)$.*

G_7**:** In this game, the challenge ciphertext is generated as

$$C_1^* \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1 p_2}, \qquad C_2^* = C_1^{*1/\tilde{\gamma}}, \qquad \boxed{C_0^* = M_\beta \oplus K}$$

where $K \xleftarrow{\mathrm{R}} \{0,1\}^\rho$. In order to prove that G_6 and G_7 are statistically close, we only need to check the following terms in G_6:

$$C_0^* = \mathsf{H}(e(C_1^*, U_0)) = \mathsf{H}(e(g^{s\cdot\gamma}, u_0) \cdot \boxed{e(g_2^{\omega_2}, g_2^{t_0})})$$
$$K_{0,1} = u_1 \cdot u_0 \cdot \boxed{g_2^{t_{0,1}+t_0}} \cdot X_{3,0,1}, \ \ldots, \ K_{0,q} = u_q \cdot u_0 \cdot \boxed{g_2^{t_{0,q}+t_0}} \cdot X_{3,0,q}$$

for some $\omega_2 \in \mathbb{Z}_N$. We emphasize that t_0 and $t_{0,1}, \ldots, t_{0,q}$ only appear in the above terms (labelled by the boxes) and $\{t_0,\ t_{0,1}+t_0,\ \ldots,\ t_{0,q}+t_0\}$ are uniformly distributed over $\mathbb{Z}_{p_2}^{q+1}$. This means that, conditioned on $\mathscr{A}$'s view, $e(C_1^*, U_0)$ still has $\log(p_2)$ bits of min-entropy when C_1^* has a non-trivial $\mathbb{G}_{p_2}$ component (i.e., $\omega_2 \neq 0 \bmod p_2$). Therefore we can conclude as in Section 3.3 that $|\Pr[E_6] - \Pr[E_7]| \leq 1/p_2 + 1/2^\lambda$.

It is not hard to observe that the challenge ciphertext reveals nothing about $\beta \in \{0,1\}$ in G_7. Thus we have $\Pr[E_7] = 1/2$. Combining all the above together, we may prove the theorem.

Proofs of Lemmas

Proof (of Lemma 4). The reduction $\mathscr{B}_1$ receives an instance $(\mathcal{G}_{\mathrm{pub}}, g_1, g_3, T)$ of DS1 and simulates the sid-cpa game to $\mathscr{A}$ as follows.

Setup. Received the challenge set S^* and threshold τ^* from $\mathscr{A}$, algorithm $\mathscr{B}_1$ samples $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and computes $\gamma = \tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)$. It sets $g = g_1$, picks $u_0 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ (taking g_1 as a generator) and computes $G_i = g^{\alpha^i}$ for $i \in [2n-1]$. $\mathscr{B}_1$ chooses $\mathsf{H} : \mathbb{G}_T \to \{0,1\}^\rho$, prepares $U_0 = u_0 \cdot X_{3.0}$ where $X_{3,0} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ and returns the following public parameters to $\mathscr{A}$.

$$\Big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^\gamma,\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ e(g,U_0)^\gamma,\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\Big)$$

where $d_1, \ldots, d_{n-1} \in \mathbb{Z}_N$ are selected arbitrarily.

Key Extraction Phase. Upon a key extraction query on S_y of size ℓ_y, the reduction $\mathscr{B}_1$ picks $u_y \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ (using $g = g_1$ as the generator), $X_{3,1,y}, \ldots, X_{3,\ell_y,y}, X'_{3,1,y}, \ldots, X'_{3,n-1,y}, X_{3,0,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ (using g_3 as the generator) and responds the query with

$$\big(K_{i,y} = u_y^{\frac{\gamma}{\alpha+\mathsf{id}_{i,y}}} \cdot X_{3,i,y}\big)_{i=1}^{\ell_y}, \quad \big(K'_{i,y} = u_y^{\alpha^i} \cdot X'_{3,i,y}\big)_{i=1}^{n-1}, \quad K_{0,y} = u_y \cdot U_0 \cdot X_{3,0,y},$$

because both α and γ are known to $\mathscr{B}_1$.

Challenge. The reduction algorithm receives two messages $M_0, M_1 \in \{0,1\}^\rho$, it picks a random bit $\beta \xleftarrow{\mathrm{R}} \{0,1\}$ and returns $\mathsf{CT}^* = (C_0^*, C_1^*, C_2^*)$ where

$$C_1^* = T, \quad C_2^* = (C_1^*)^{1/\tilde{\gamma}}, \quad C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0)).$$

Guess. Finally, $\mathscr{A}$ returns its guess β' and $\mathscr{B}_1$ returns 1 if and only if $\beta = \beta'$.

Observe that the distribution of CT^* is as in game G_2 if $T \in \mathbb{G}_{p_1}$ and identical to G_3 if $T \in \mathbb{G}_{p_1 p_2}$. This proves the lemma. □

Proof (of Lemma 5). On input an instance $(\mathcal{G}_{\mathrm{pub}}, g_1, g_3, h_{12}, h_{23}, T)$ of DS2 problem, the reduction $\mathscr{B}_2$ simulates the sid-cpa game as follows.

Setup. $\mathscr{A}$ commits to the challenge set S^* and the challenge threshold τ^*. $\mathscr{B}_2$ chooses $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and compute $\gamma = \tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)$. By setting $g = g_1$, $\mathscr{B}_2$ can compute $G_i = g^{\alpha^i}$ for each $i \in [2n-1]$. It sets $U_0 = u_0 \cdot X_{3.0}$ where $u_0 \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ and $X_{3,0} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$ and returns the public parameters

$$\left(\mathcal{G}_{\mathrm{pub}},\ g,\ g^{\gamma},\ \left(G_i = g^{\alpha^i}\right)_{i=1}^{2n-1},\ e(g,U_0)^{\gamma},\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\right)$$

where $d_1, \ldots, d_{n-1} \in \mathbb{Z}_N$ are dummy identities and H is a universal hash function as required. $\mathscr{B}_2$ also choose $\alpha_1, \ldots, \alpha_{k-1} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$.

Key Extraction Phase. When receiving the y-th query $S_y \subseteq \mathcal{I}$ of size ℓ_y, $\mathscr{B}_2$ considers two cases:

- if $k \leq \ell_y + n$, $\mathscr{B}_2$ picks $\mu_y, \tilde{r}_{1,y}, \ldots, \tilde{r}_{k-1,y} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and $\tilde{X}_{3,1,y}, \ldots, \tilde{X}_{3,\ell_y,y}$, $\tilde{X}'_{3,1,y}, \ldots, \tilde{X}'_{3,n-1,y}, \tilde{X}_{3,0,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. The secret key is computed as

$$\begin{aligned}
&\left(K_{i,y} = T^{\mu_y \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot (h_2 h_3)^{\tilde{\gamma} \sum_{j=1}^{k-1} \frac{p_{S^*,\tau^*}(\alpha_j)}{\alpha_j + \mathsf{id}_{i,y}} \tilde{r}_{j,y}} \cdot \tilde{X}_{3,i,y}\right)_{i=1}^{\ell_y},\\
&\left(K'_{i,y} = T^{\mu_y \alpha^i} \cdot (h_2 h_3)^{\sum_{j=1}^{k-1} \alpha_j^i \tilde{r}_{j,y}} \cdot \tilde{X}'_{3,i,y}\right)_{i=1}^{n-1},\\
&K_{0,y} = T^{\mu_y} \cdot (h_2 h_3)^{\sum_{j=1}^{k-1} \tilde{r}_{j,y}} \cdot U_0 \cdot \tilde{X}_{3,0,y},
\end{aligned}$$

- if $k > \ell_y + n$, $\mathscr{B}_2$ picks $u_y \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ using g_1 as the generator, $\tilde{r}_{1,y}, \ldots, \tilde{r}_{\ell_y+n,y} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and $\tilde{X}_{3,1,y}, \ldots, \tilde{X}_{3,\ell_y,y}$, $\tilde{X}'_{3,1,y}, \ldots, \tilde{X}'_{3,n-1,y}$, $\tilde{X}_{3,0,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. The secret key can be computed as

$$\begin{aligned}
&\left(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot (h_2 h_3)^{\tilde{\gamma} \sum_{j=1}^{\ell_y+n} \frac{p_{S^*,\tau^*}(\alpha_j)}{\alpha_j + \mathsf{id}_{i,y}} \tilde{r}_{j,y}} \cdot \tilde{X}_{3,i,y}\right)_{i=1}^{\ell_y},\\
&\left(K'_{i,y} = u_y^{\alpha^i} \cdot (h_2 h_3)^{\sum_{j=1}^{\ell_y+n} \alpha_j^i \tilde{r}_{j,y}} \cdot \tilde{X}'_{3,i,y}\right)_{i=1}^{n-1},\\
&K_{0,y} = u_y \cdot (h_2 h_3)^{\sum_{j=1}^{\ell_y+n} \tilde{r}_{j,y}} \cdot U_0 \cdot \tilde{X}_{3,0,y},
\end{aligned}$$

Challenge. In the challenge phase, $\mathscr{A}$ chooses two messages $M_0, M_1 \in \{0,1\}^{\rho}$. The reduction $\mathscr{B}_2$ picks $\beta \xleftarrow{\mathrm{R}} \{0,1\}^n$ and returns the challenge ciphertext

$$C_1^* = h_{12}, \qquad C_2^* = (C_1^*)^{1/\tilde{\gamma}}, \qquad C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0)).$$

Guess. When $\mathscr{A}$ has its guess β', $\mathscr{B}_2$ returns 1 if and only if $\beta = \beta'$.

Let $g_2 \in \mathbb{G}_{p_2}$ be a generator of $\mathbb{G}_{p_2}$, we can write $h_2 h_3 = g_2^{\omega_2} h_3$ and $T = g_1^{\omega_1} \cdot g_2^{\omega_2^*} \cdot T_3$ where $\omega_2, \omega_1, \xleftarrow{\mathrm{R}} \mathbb{Z}_N$, ω_2^* is either a random element in $\mathbb{Z}_N$ or equals 0, and h_3, T_3 are uniformly distributed over $\mathbb{G}_{p_3}$. In the key extraction phase, the simulation for the second case is correct where $\mathscr{B}_2$ implicitly sets

$$r_{1,y} = \omega_2 \cdot \tilde{r}_{1,y},\ \ldots,\ r_{\ell_y+n,y} = \omega_2 \cdot \tilde{r}_{\ell_y+n,y}$$

for S_y; for the first case, $\mathscr{B}_2$ implicitly sets

$$u_y = g_1^{\omega_1 \mu_y},\ r_{1,y} = \omega_2 \cdot \tilde{r}_{1,y},\ \ldots,\ r_{k-1,y} = \omega_2 \cdot \tilde{r}_{k-1,y},\ r_{k,y} = \omega_2^* \mu_y \bmod p_2.$$

Note that u_y only reveals $\mu_y \bmod p_1$. Therefore when $\omega_2^* \neq 0$ (i.e., $T \in \mathbb{G}_{p_1p_2p_3}$), $r_{k,y}$ is uniformly distributed over $\mathbb{Z}_N$ and the simulation is identical to $\mathsf{G}_{4.k.0}$; otherwise, when $\omega_2^* = 0$ (i.e., $T \in G_{p_1p_3}$), we have $r_{k,y} = 0$ and the simulation is as $\mathsf{G}_{4.(k-1).1}$. This readily proves the lemma. □

Proof (of Lemma 6). For convenience, we discard the subscript $y \in [q]$. We note that our analysis can be applied to all $\mathbf{B}_1, \ldots, \mathbf{B}_q$. Let $(S^* = (\mathsf{id}_1^*, \ldots, \mathsf{id}_{\ell^*}^*), \tau^*)$ be the challenge set and threshold while $S = (\mathsf{id}_1, \ldots, \mathsf{id}_\ell)$ be the set associated with the key we are looking at. According to the security model, the size of $S \cap S^*$ must be smaller than τ^*. W.L.O.G, we may let $\tau < \tau^*$ be the size and assume

$$\mathsf{id}_1 = \mathsf{id}_1^*, \ \ldots, \ \mathsf{id}_\tau = \mathsf{id}_\tau^*$$

(In fact this can be achieved via re-ordering.) We define the polynomials

$$p_{-i}(x) = p_{S^*,\tau^*}(x)/(x + \mathsf{id}_i) \quad \text{for all} \ \ i \in [\tau].$$

We will argue the following matrix is invertible w.h.p when $\alpha_1, \ldots, \alpha_{\ell+n} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$.

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & \cdots\cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{\ell+n} \\ \alpha_1^2 & \alpha_2^2 & \cdots\cdots & \alpha_{\ell+n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots\cdots & \alpha_{\ell+n}^{n-1} \\ \tilde{\gamma} \cdot p_{-1}(\alpha_1) & \tilde{\gamma} \cdot p_{-1}(\alpha_2) & \cdots\cdots & \tilde{\gamma} \cdot p_{-1}(\alpha_{\ell+n}) \\ \vdots & \vdots & & \vdots \\ \tilde{\gamma} \cdot p_{-\tau}(\alpha_1) & \tilde{\gamma} \cdot p_{-\tau}(\alpha_2) & \cdots\cdots & \tilde{\gamma} \cdot p_{-\tau}(\alpha_{\ell+n}) \\ \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_1)}{\alpha_1 + \mathsf{id}_{\tau+1}} & \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_2)}{\alpha_2 + \mathsf{id}_{\tau+1}} & \cdots\cdots & \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_{\ell+n})}{\alpha_{\ell+n} + \mathsf{id}_{\tau+1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_1)}{\alpha_1 + \mathsf{id}_\ell} & \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_2)}{\alpha_2 + \mathsf{id}_\ell} & \cdots\cdots & \frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha_\ell + n)}{\alpha_{\ell+n} + \mathsf{id}_\ell} \end{pmatrix}.$$

Let

$$q(x) = \textstyle\prod_{i \in [\tau+1,\ell]}(x + \mathsf{id}_i) \ \ \text{and} \ \ q_{-i}(x) = q(x)/(x + \mathsf{id}_i) \ \text{for all} \ \ j \in [\tau + 1, \ell].$$

We may equivalently study the following matrix, denoted by $\hat{\mathbf{B}}$, which is obtained from $\mathbf{B}$ by multiplying the j-th column by $q(\alpha_j)$ for $j \in [\ell + n]$ and multiplying each of the last $\ell - \tau$ rows by $1/\tilde{\gamma}$.

$$\begin{pmatrix} q(\alpha_1) & q(\alpha_2) & \cdots\cdots & q(\alpha_{\ell+n}) \\ \alpha_1 q(\alpha_1) & \alpha_2 q(\alpha_2) & \cdots\cdots & \alpha_\ell q(\alpha_{\ell+n}) \\ \alpha_1^2 q(\alpha_1) & \alpha_2^2 q(\alpha_2) & \cdots\cdots & \alpha_\ell^2 q(\alpha_{\ell+n}) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} q(\alpha_1) & \alpha_2^{n-1} q(\alpha_2) & \cdots\cdots & \alpha_\ell^{n-1} q(\alpha_{\ell+n}) \\ p_{-1}(\alpha_1) q(\alpha_1) & p_{-1}(\alpha_2) q(\alpha_2) & \cdots\cdots & p_{-1}(\alpha_{\ell+n}) q(\alpha_{\ell+n}) \\ \vdots & \vdots & & \vdots \\ p_{-\tau}(\alpha_1) q(\alpha_1) & p_{-\tau}(\alpha_2) q(\alpha_2) & \cdots\cdots & p_{-\tau}(\alpha_{\ell+n}) q(\alpha_{\ell+n}) \\ p_{S^*,\tau^*}(\alpha_1) q_{-(\tau+1)}(\alpha_1) & p_{S^*,\tau^*}(\alpha_2) q_{-(\tau+1)}(\alpha_2) & \cdots\cdots & p_{S^*,\tau^*}(\alpha_\ell) q_{-(\tau+1)}(\alpha_{\ell+n}) \\ \vdots & \vdots & & \vdots \\ p_{S^*,\tau^*}(\alpha_1) q_{-\ell}(\alpha_1) & p_{S^*,\tau^*}(\alpha_2) q_{-\ell}(\alpha_2) & \cdots\cdots & p_{S^*,\tau^*}(\alpha_\ell) q_{-\ell}(\alpha_{\ell+n}) \end{pmatrix}.$$

Following the idea of Chase and Meiklejohn [23], it is sufficient to argue the following polynomials (in x) are linearly independent.

$$\begin{array}{l} q(x), xq(x), \ldots, x^{n-1}q(x), p_{-1}(x)q(x), \ldots, p_{-\tau}(x)q(x), \\ p_{S^*,\tau^*}(x)q_{-(\tau+1)}(x), \ldots, p_{S^*,\tau^*}(x)q_{-\ell}(x). \end{array} \tag{4}$$

Let us assume that there exist coefficients $a_0, a_1, \ldots, a_{n-1}$, $b_1, \ldots, b_\tau$, $c_{\tau+1}, \ldots, c_\ell \in \mathbb{Z}_N$ such that

$$C(x) = \sum_{i\in[0,n-1]} a_i x^i q(x) + \sum_{i\in[\tau]} b_i p_{-i}(x)q(x) + \sum_{i\in[\tau+1,\ell]} c_i p(x) q_{-i}(x)$$

is a zero polynomial. We prove that all these coefficients are zero in two steps.

Step 1. For all $i \in [\tau+1, \ell]$, we have

$$C(-\mathsf{id}_i) = c_i p(-\mathsf{id}_i) q_{-i}(-\mathsf{id}_i) = 0,$$

because $-\mathsf{id}_i$ is a common root of $q(x)$ and $q_{-j}(x)$ with $j \neq i$. Since $-\mathsf{id}_i$ is not a root of $p(x)$ and $q_{-i}(x)$, we can deduce that $c_i = 0$.

Step 2. It remains to show that all a_i and b_i are zero. We should prove that

$$1, x, \ldots, x^{n-1}, p_{-1}(x), \ldots, p_{-\tau}(x) \tag{5}$$

are linearly independent. To this end, let us take a closer look at the polynomials $p_{-i}(x)$ with $i \in [\tau]$. For each i, we may rewrite

$$p_{-i}(x) = \underbrace{\prod_{j\in[\tau]\setminus\{i\}} (x + \mathsf{id}_j)}_{\hat{p}_{-i}(x)} \cdot \underbrace{\prod_{j\in[\tau+1,\ell^*]} (x + \mathsf{id}_j^*) \cdot \prod_{i\in[n+\tau^*-1-\ell^*]} (x + d_i)}_{\tilde{p}(x)}.$$

We rely on two observations: (1) $\tilde{p}(x)$ divides all $p_{-i}(x)$ and $\deg(\tilde{p}) = n + \tau^* - 1 - \tau \geq n$; (2) $\hat{p}_{-1}(x), \ldots, \hat{p}_{-\tau}(x)$ are linearly independent polynomials of degree $\tau - 1$. The second observation means $\hat{p}_{-1}(x), \ldots, \hat{p}_{-\tau}(x)$ form a basis of all polynomial of degree at most $\tau - 1$. This means that proving the independence of (5) is equivalent to proving the independence of

$$1, x, \ldots, x^{n-1}, \tilde{p}(x), x\tilde{p}(x), \ldots, x^{\tau-1}\tilde{p}(x) \tag{6}$$

because $1, x, x^2, \ldots, x^{\tau-1}$ also form a basis of the linear space of all polynomials of degree $\leq \tau - 1$. From the first observation, we can see that

$$\deg(\tilde{p}(x)) = n + \epsilon,\ \deg(x\tilde{p}(x)) = n + 1 + \epsilon,\ \ldots,\ \deg(x^{\tau-1}\tilde{p}(x)) = n + \tau - 1 + \epsilon$$

for some non-negative integer ϵ. This immediately derives that the $\ell + n$ polynomials in Eq.(6) are linearly independent and so are the polynomials in Eq.(5).

Combining this two steps, we prove that polynomials in Eq.(4) are linearly independent. Since $\det(\hat{\mathbf{B}})$ is a polynomial in $\alpha_1, \ldots, \alpha_{\ell+n}$ of degree at most $(\ell + 2n)^2$, the Schwartz-Zippel implies $\det(\hat{\mathbf{B}}) = 0$ with the probability bounded by $(\ell + 2n)^2/p_2$ and so does the event $\det(\mathbf{B}) = 0$ when sampling $\alpha_1, \ldots, \alpha_{\ell+n} \xleftarrow{\mathrm{R}} \mathbb{Z}_{p_2}$. By the union bound, we immediately prove the lemma. □

Proof (of Lemma 7). On input an instance $(\mathcal{G}_{\mathrm{pub}}, g_1, g_3, h_{12}, h_{23}, T)$ of DS2 problem, the reduction $\mathscr{B}_2$ simulates the sid-cpa game as follows.

Setup. $\mathscr{A}$ commits to the challenge set S^* and the challenge threshold τ^*. $\mathscr{B}_2$ chooses $\alpha, \tilde{\gamma} \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ and compute $\gamma = \tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)$. By setting $g = g_1$, $\mathscr{B}_2$ can compute $G_i = g^{\alpha^i}$ for each $i \in [2n-1]$. $\mathscr{B}_2$ defines $U_0 = T$ and returns the public parameters

$$\Big(\mathcal{G}_{\mathrm{pub}},\ g,\ g^{\gamma},\ \big(G_i = g^{\alpha^i}\big)_{i=1}^{2n-1},\ e(g, U_0)^{\gamma},\ (d_i)_{i=1}^{n-1},\ \mathsf{H}\Big)$$

where $d_1, \ldots, d_{n-1} \in \mathbb{Z}_N$ are dummy identities and H is a universal hash function as required.

Key Extraction Phase. When receiving the y-th query $S_y \subseteq \mathcal{I}$ of size ℓ_y, $\mathscr{B}_2$ samples $u_y \xleftarrow{\mathrm{R}} \mathbb{G}_{p_1}$ (using $g = g_1$), $\tilde{t}_{0,y}, \tilde{t}'_{1,y} \ldots, \tilde{t}'_{n-1,y}, \tilde{t}_{1,y}, \ldots, \tilde{t}_{\ell_y,y} \in \mathbb{Z}_N$ and $\tilde{X}_{3,0,y}, \tilde{X}'_{3,1,y}, \ldots, \tilde{X}'_{3,n-1,y}, \tilde{X}_{3,1,y}, \ldots, \tilde{X}_{3,\ell_y,y} \xleftarrow{\mathrm{R}} \mathbb{G}_{p_3}$. It then returns the secret key

$$\Big(K_{i,y} = u_y^{\frac{\tilde{\gamma} \cdot p_{S^*,\tau^*}(\alpha)}{\alpha + \mathsf{id}_{i,y}}} \cdot (h_2 h_3)^{\tilde{t}_{i,y}} \cdot \tilde{X}_{3,i,y}\Big)_{i=1}^{\ell_y},\ \Big(K'_{i,y} = u_y^{\alpha^i} \cdot (h_2 h_3)^{\tilde{t}'_{i,y}} \cdot \tilde{X}'_{3,i,y}\Big)_{i=1}^{n-1},$$

$$K_{0,y} = u_y \cdot (h_2 h_3)^{\tilde{t}_{0,y}} \cdot U_0 \cdot \tilde{X}_{3,0,y}.$$

Challenge. In the challenge phase, $\mathscr{A}$ chooses two messages $M_0, M_1 \in \{0,1\}^{\rho}$. The reduction $\mathscr{B}_2$ picks $\beta \xleftarrow{\mathrm{R}} \{0,1\}^n$ and returns the challenge ciphertext

$$C_1^* = h_{12}, \qquad C_2^* = (C_1^*)^{1/\tilde{\gamma}}, \qquad C_0^* = M_\beta \oplus \mathsf{H}(e(C_1^*, U_0)).$$

Guess. When $\mathscr{A}$ has its guess β', $\mathscr{B}_2$ returns 1 if and only if $\beta = \beta'$.

As before we can write $h_2 h_3 = g_2^{\omega_2} h_3$ and $T = g_1^{\omega_1} \cdot g_2^{\omega_2^*} \cdot T_3$ where $g_2 \in \mathbb{G}_{p_2}$ is a generator of $\mathbb{G}_{p_2}$, $\omega_2, \omega_1, \xleftarrow{\mathrm{R}} \mathbb{Z}_N$, ω_2^* is either a random element in $\mathbb{Z}_N$ or equals 0, and h_3, T_3 are uniformly distributed over $\mathbb{G}_{p_3}$. In the key extraction phase, $\mathscr{B}_2$ implicitly sets

$$t_{0,y} = \omega_2 \cdot \tilde{t}_{0,y}, t'_{1,y} = \omega_2 \cdot \tilde{t}'_{1,y},\ \ldots,\ t'_{n-1,y} = \omega_2 \cdot \tilde{t}'_{n-1,y},$$

$$t_{1,y} = \omega_2 \cdot \tilde{t}_{1,y},\ \ldots,\ t_{\ell_y,y} = \omega_2 \cdot \tilde{t}_{\ell_y,y}.$$

Because we implicitly set $t_0 = \omega_2^*$, when $\omega_2^* \neq 0$ (i.e., $T \in \mathbb{G}_{p_1 p_2 p_3}$), the simulation is identical to G_6; otherwise, when $\omega_2^* = 0$ (i.e., $T \in G_{p_1 p_3}$), the simulation is as G_5. This proves the lemma. □